LATTICE-BASED CODING SCHEMES FOR WIRELESS RELAY NETWORKS

A Dissertation

by

NIHAT ENGIN TUNALI

Submitted to the Office of Graduate and Professional Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Chair of Committee,	Krishna R. Narayanan
Committee Members,	Henry D. Pfister
	Srinivas Shakkottai
	Anxiao (Andrew) Jiang
Head of Department,	Chanan Singh

December 2014

Major Subject: Electrical Engineering

ABSTRACT

Compute-and-forward is a novel relaying paradigm in wireless communications in which relays in a network directly compute or decode functions of signals transmitted from multiple transmitters and forward them to a central destination. In this dissertation, we study three problems related to compute-and-forward.

In the first problem, we consider the use of lattice codes for implementing a compute-and-forward protocol in wireless networks when channel state information is not available at the transmitter. We propose the use of lattice codes over Eisenstein integers and we prove the existence of a sequence of lattices over Eisenstein integers which are good for quantization and achieve capacity over an additive white Gaussian noise (AWGN) channel. Using this, we show that the information rates achievable with nested lattice codebooks over Eisenstein integers are higher than those achievable with nested lattice codebooks over integers considered by Nazer and Gastpar in [6] in the average sense. We also propose a separation-based framework for compute-and-forward that is based on the concatenation of a non-binary linear code with a modulation scheme derived from the ring of Eisenstein integers, which enables the coding gain and shaping gain to be separated, resulting in significantly higher theoretically achievable computation rates.

In the second problem, we construct lattices based on spatially-coupled low-density parity check (LDPC) codes and empirically show that such lattices can approach the Poltyrev limit very closely for the point-to-point unconstrained AWGN channel. We then employ these lattices to implement a compute-and-forward protocol and empirically show that these lattices can approach the theoretically achievable rates closely.

In the third problem, we present a new coding scheme based on concatenating a newly introduced class of lattice codes called convolutional lattice codes with LDPC codes, which we refer to as concatenated convolutional lattice codes (CCLS) and study their application to compute-and-forward (CF). The decoding algorithm for CCLC is based on an appropriate combination of the stack decoder with a message passing algorithm, and is computationally much more efficient than the conventional decoding algorithm for convolutional lattice codes. Simulation results show that CCLC can approach the point-to-point uniform input AWGN capacity very closely with soft decision decoding. Also, we show that they possess the required algebraic structure which makes them suitable for recovering linear combinations (over a finite field) of the transmitted signals in a multiple access channel. This facilitates their use as a coding scheme for the compute-and-forward paradigm. Simulation results show that CCLC can approach theoretically achievable rates very closely when implemented for the compute-and-forward.

ACKNOWLEDGEMENTS

First and foremost, I would like to thank my advisor, Professor Krishna Narayanan, who has guided me throughout my graduate studies. He has been a wonderful mentor and teacher. His broad and in-depth knowledge and his enthusiasm has helped me propose solutions to a variety of problems. Moreover, during some of the hardships that my family and I have been through, he has supported me immensely and has been a friend to me.

I would also like to thank Professor Henry Pfister for the many fruitful discussions we had on coding theory. He has given me countless valuable advice when I was in the job market, which I greatly appreciate. I would like to thank my other committee members as well. Professor Srinivas Shakkottai's Game Theory lectures were very interesting and provided me with insight outside of my area of research. Professor Andrew Jiang has asked very constructive questions during my preliminary exam and he has also suggested a variety of resources to study coding for storage. I would also like to thank Professor Joseph Jean Boutros for his valuable input on a variety of problems that we studied together.

I would like to thank my friend and office mate Jerry Huang. He has supported me during hard times and we have also had lots of fun together. Also, his endless motivation and his systematic intelligent approach to tackling problems has taught me a lot during these past years. There is no doubt that he will be a great faculty member in the following years. I would also like to thank Brett Hern, Amir Salimi, Santhosh Kumar, Yung-Yih Jian, Avinash Vem, Fatemeh Hamidi Sepehr, Armin Banaei, Parimal Parag, and Nariman Rahimian for all the interesting discussions and fun times we had.

Many thanks to my parents who have loved me, been there for me, and endlessly supported me since the day I was born. I would also like to thank my parents-in-law, who have helped me and my wife take care of our newborn baby for several months and supported me. I especially would like to thank my beloved wife Miray for her endless love and for giving birth to our lovely daughter Defne, who means the world to me.

TABLE OF CONTENTS

Page

LIST OF FIGURES

FIGURE Page

LIST OF TABLES

TABLE Page

1. INTRODUCTION

Since Shannon's signature paper, "A mathematical theory of communication" was published in 1948, one of the main focuses of coding theory has been to design coding schemes with reasonable encoding and decoding complexities that approach the Shannon limit for the point-to-point additive white Gaussian noise (AWGN) channel. After nearly six decades of hard work by many researchers, a variety of error correcting codes such as Turbo codes, LDPC codes, and most recently Polar codes, have been discovered which approach the Shannon limit for the point-to-point AWGN channel.

In the last three decades, the widespread use of the internet and cell-phones, particularly smart phones, has led to a substantial increase in the amount of data exchanged over wireless networks. Unlike the point-to-point channel, the best achievable rates for even the simplest wireless network setups, such as the two user interference channel, are not known. Moreover, it is not known whether the utilization of coding schemes that are known to approach the Shannon limit for the point-to-point channel would result in the highest achievable rates for wireless networks. These open problems have motivated researchers to move beyond known paradigms for the point-to-point channel and design information forwarding strategies and coding schemes that take advantage of certain properties of the wireless medium, such as superposition and the ability to broadcast in order to achieve higher exchange rates and combat path loss.

In this dissertation, we will focus on a special case of wireless networks which are referred to as wireless relay networks. A wireless relay network consists of a set of transmitter nodes and a set of relays. Typically, direct communication between

transmitter nodes are restricted and communication is facilitated through the relays. One of the most commonly used system models for wireless relay networks is the additive white Gaussian noise (AWGN) relay network. In the AWGN relay network, there is also a final destination node which all relays transmit to. This destination node's goal is to determine the individual messages of the transmitter nodes. We provide a detailed description of the AWGN relay network in section 2.3.

A variety of information forwarding strategies can be used in an AWGN relay network. Amplify-and-forward is an information forwarding strategy where the relays scale their observation in order to satisfy the power constraint and forward it to the final destination node [40]. The main drawback of amplify-and-forward is the propagation of noise throughout the network. Decode-and-forward is another information forwarding strategy where the relays individually decode to the messages transmitted from the transmitter nodes and re-encode them for collaborative transmission [41]. The main drawback of decode-and-forward is the limitation of the achievable rates by interference.

In this dissertation, we will focus on compute-and-forward (CF), which is a more recently introduced information forwarding paradigm in wireless networks [6]. In compute-and-forward, relays directly decode to functions of transmitted messages from the transmitter nodes. These functions are chosen carefully such that when the central destination receives them, it is able to determine each transmitted message individually. One way to choose these functions would be to decode to a linear integer combination of transmitted messages. For this choice of functions, it is highly desirable for a code to have an additive group property under real additions. Lattice codes are a class of codes that have this property and therefore they are a perfect candidate for implementing compute-and-forward.

A variety of open problems exist in the compute-and-forward framework for

the AWGN relay network. One of these open problems is that the performance of lattice codes with reasonable encoding and decoding complexities and how close they approach theoretically achievable rates for this framework have not been well-investigated. Another open problem is that it is not known whether it would be possible to recover linear combinations that are different from integer linear combinations that would result in higher achievable rates. A third open problem is that it is not known whether it would be possible to design a more practically implementable framework for compute-and-forward with achievable rates comparable to theoretically achievable rates.

In this dissertation, we thoroughly study these three problems. We show that by choosing a different construction of lattices and choosing Eisentein integers for obtaining linear combinations of transmitted signals, higher information rates can be achieved than what was stated in [6]. Also, we propose a separation-based framework for compute-and-forward where the demodulation and decoding is separated and show that this framework can achieve higher computation rates. We then design lattice codes with reasonable encoding and decoding complexities that approach the achievable computation rates stated in [6] and [24].

1.1 Organization

The rest of this dissertation is organized as follows. In Chapter 2, we specify the notation that will be used throughout this dissertation and provide some background on lattices and the lattice-based compute-and-forward framework proposed in [6] and [24]. In Chapter 3, we first show that there exist lattices over Eisenstein integers that are simultaneously good for quantization and good for AWGN channel coding and then we adapt Nazer and Gastpar's framework in [6] to lattices over Eisenstein integers, i.e., decoding to a linear Eisenstein integer combination. Sim-

ulation results show that lattices over Eisenstein integers can achieve substantially higher computation rates than lattices over integers for certain channel realizations and in the average sense. We then introduce a separation-based coding scheme for compute-and-forward based on lattice codes obtained from lattices over Eisenstein integers built with Construction A, where the demodulation and decoding are implemented separately. Simulation results show that this coding scheme can achieve higher computation rates than Nazer and Gastpar's coding scheme over Eisenstein integers as the field size increases. In Chapter 4, we construct lattice codes from Spatially-Coupled LDPC codes, which we refer to as SCLDA codes and show that they approach the Poltyrev limit very closely. Motivated by this result, we implement SCLDA code for our separation-based coding scheme for compute-and-forward and show that we can closely approach theoretically achievable rates. In Chapter 5, we introduce a new class of lattice codes obtained from concatenating a newly introduced class of lattice codes known as convolutional lattice codes [13], with interleaved Low Density Parity Check (LDPC) codes, which we refer to as concatenated convolutional lattice codes (CCLC). Simulation results show that CCLC can achieve good error correcting performance with less complex decoders for the point-to-point channel and can be effectively implemented for compute-and-forward without an increase in the complexity of the decoder. In Chapter 6, we discuss some of the potential future work of our studies we mentioned in Chapters 3, 4, and 5.

2. BACKGROUND

In this chapter, we first specify the notation that will be used throughout this dissertation. We then provide some background on lattices and nested lattice codes and some important properties of lattices that lay the foundation for our contributions. Finally, we describe the AWGN relay network in detail and cover the lattice-based framework for compute-and-forward proposed in [24] and [6].

2.1 Notational convention

Throughout this dissertation, we use $\mathbb{R}$ to denote the field of real numbers, $\mathbb{C}$ to denote the field of complex numbers, and $\mathbb{F}_q$ to denote a finite field of size q. $\mathbb{Z}$, $\mathbb{Z}[i]$, and $\mathbb{Z}[\omega]$ are used to denote the set of integers, Gaussian integers, and Eisenstein integers, respectively. We use underlined variables to denote vectors and boldface uppercase variables to denote matrices, e.g., $\underline{x}$ and $\mathbf{X}$, respectively. We denote the j^{th} column of a matrix $\mathbf{X}$ as $\mathbf{X}_j$, the i^{th} row of a matrix $\mathbf{X}$ as $\underline{x}^i$,the element at the i^{th} row and j^{th} column of a matrix $\mathbf{X}$ as $\underline{x}_{i,j}$, and the i^{th} element of a vector $\underline{x}$ as x_i. We denote the vector that consists of all the elements between indices (i, j) and $(i, j + L)$ in a matrix $\mathbf{X}$ as $x_{i,j}^{i,j+L}$. The distinction between a row or a column vector can be understood from the context. Also, we use superscript T to denote the transpose operation, e.g., $\underline{x}^T$ and $\mathbf{X}^T$. We use superscript H to denote the Hermitian operation, e.g., $\underline{x}^H$ and $\mathbf{X}^H$. We denote addition and multiplication over a finite field as $\oplus$ and $\cdot$, respectively. We denote the Euclidean metric as $\| \ \|$, the discrete convolution operation as $\star$, the cardinality of a set $\mathcal{S}$ as $|\mathcal{S}|$, and a ball with center x and radius r as $\mathcal{B}(x, r)$.. Also,. We define $\log^+(x) \triangleq \max(\log(x), 0)$. We denote the all zero vector in $\mathbb{R}^n$ as $\underline{0}$ and the $n \times n$ identity matrix as $\mathbf{I}$. We denote the volume of a bounded region $E \in \mathbb{R}^n$ as $\mathrm{Vol}\,(E)$ and denote the n-dimensional

sphere of radius r centered at $\underline{0}$ as $\mathcal{B}(r) \triangleq \{\underline{s} \ : \ \|\underline{s}\| \leq r\}$. For a discrete set S, we denote $S' \triangleq S \setminus 0$.

2.2 Lattices, nested lattice codes, and Construction A

Definition 1 (Lattice over $\mathbb{Z}$)**.** *An n-dimensional lattice over natural integers, $\Lambda^{(n)}$, is a discrete set of points in $\mathbb{R}^n$ such that $\Lambda^{(n)}$ is a discrete additive subgroup of $\mathbb{R}^n$ with rank k where $k \leq n$. Such a lattice can be generated via a full rank generator matrix $\mathbf{B} \in \mathbb{R}^{n \times k}$ according to*

$$\Lambda^{(n)} = \left\{\underline{\lambda} = \mathbf{B}\underline{e} : \underline{e} \in \mathbb{Z}^k\right\}. \tag{2.1}$$

In Fig. 2.1, we depict the hexagonal lattice, which is over $\mathbb{R}^2$ and has a generator matrix $\mathbf{B} = [\ 1 \ \ 0 \ ; \ \ -1/2 \ \ \sqrt{3}/2\ ]$.

For notational convenience, we shall drop the superscript in $\Lambda^{(n)}$ in this dissertation and denote n-dimensional lattices as Λ. Also, we refer to lattices over integers as $\mathbb{Z}$-lattices throughout this dissertation.

Definition 2 (Quantizer)**.** *Given a $\mathbb{Z}$-lattice Λ, a lattice quantizer with respect to Λ is a mapping, $Q_\Lambda : \mathbb{R}^n \to \Lambda$, that maps a point $\underline{s} \in \mathbb{R}^n$, to the closest lattice point in Euclidean distance:*

$$Q_\Lambda(\underline{s}) = \arg\min_{\underline{\lambda} \in \Lambda} \|\underline{s} - \underline{\lambda}\|. \tag{2.2}$$

Definition 3 (Fundamental Voronoi Region)**.** *The* fundamental Voronoi region *of a given $\mathbb{Z}$-lattice Λ, denoted as $\mathcal{V}_\Lambda$, is the set of all points in $\mathbb{R}^n$ that are quantized with respect to Λ to the all zero vector:*

$$\mathcal{V}_\Lambda = \{\underline{s} \ : \ Q_\Lambda(\underline{s}) = \underline{0}\}. \tag{2.3}$$

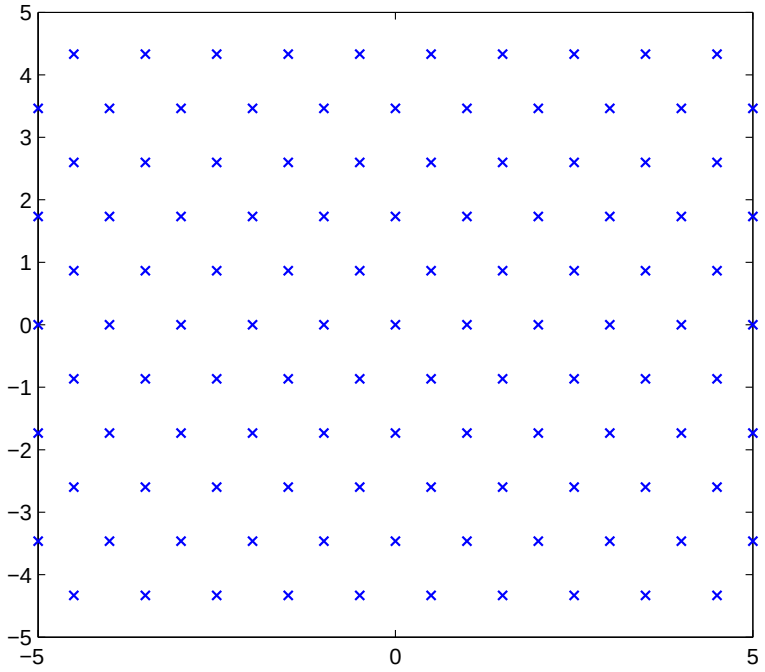

Figure 2.1: A_2 lattice

In Fig. 2.2, we depict the quantization operation and the Voronoi region of a set of lattice points. The smaller hexagons are the Voronoi regions of the lattice points, which are colored in green. Some point in $\mathbb{R}^2$ is colored in blue and as one might expect, the blue point is quantized to the lattice point which has a Voronoi region that contains it.

Definition 4 (Modulus)**.** *The* modulus *of a vector* $\underline{s} \in \mathbb{R}^n$ *with respect to a given* $\mathbb{Z}$*-lattice* Λ *is the quantization error with respect to* Λ*, denoted as* $\underline{s} \mod \Lambda$*:*

$$\underline{s} \mod \Lambda = \underline{s} - Q_\Lambda(\underline{s}). \tag{2.4}$$

Definition 5 (Covering radius)**.** *The* covering radius *of a* $\mathbb{Z}$*-lattice* Λ*, which we*

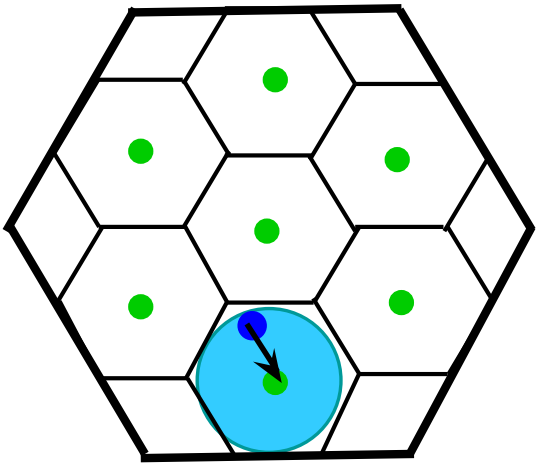

Figure 2.2: Voronoi regions and quantization

denote as r_{Λ}^{cov}*, is the smallest real number such that* $\mathbb{R}^n \subseteq \Lambda + \mathcal{B}\left(r_{\Lambda}^{cov}\right)$.

Definition 6 (Effective radius)**.** *The* effective radius *of a* $\mathbb{Z}$*-lattice* Λ*, which we denote as* r_{Λ}^{eff}*, is the real number that satisfies:*

$$Vol(\mathcal{B}\left(r_{\Lambda}^{eff}\right)) = Vol(\mathcal{V}_{\Lambda}), \tag{2.5}$$

where $Vol(\mathcal{V}_{\Lambda})$ *is referred to as the* fundamental volume *of* Λ.

We depict the covering radius and effective radius of a lattice in Fig. 2.3. In this figure, the hexagon that contains the lattice point is the Voronoi region for this lattice point. Therefore, in order to cover $\mathbb{R}^2$, the ball that has this lattice point in the center is required to contain the Voronoi region of the lattice point. Hence, it also follows that Λ, $r_{\Lambda}^{\text{cov}} \geq r_{\Lambda}^{\text{eff}}$.

Definition 7 (Second moment)**.** *The* second moment *of a* $\mathbb{Z}$*-lattice* Λ*, which we denote as* σ_{Λ}^2*, is defined as the second moment per dimension of a uniform distribution*

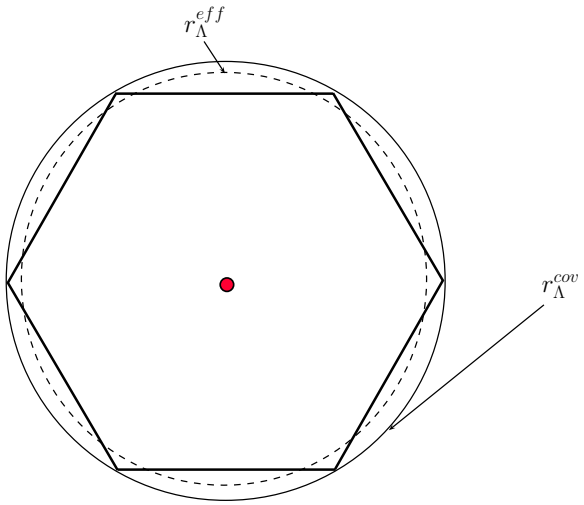

Figure 2.3: Covering radius and effective radius of a lattice

over $\mathcal{V}_\Lambda$

$$\sigma_\Lambda^2 = \frac{1}{n\,Vol(\mathcal{V}_\Lambda)} \int_{\mathcal{V}_\Lambda} \|\underline{x}\|^2 d\underline{x}. \tag{2.6}$$

Definition 8 (Normalized second moment)**.** *The* normalized second moment *of a* $\mathbb{Z}$*-lattice* Λ*, which we denote as* $G(\Lambda)$*, is defined as:*

$$G(\Lambda) = \frac{\sigma_\Lambda^2}{(Vol(\mathcal{V}_\Lambda))^{2/n}} \tag{2.7}$$

Definition 9 (Goodness for covering)**.** *A sequence of lattices* $\Lambda^{(n)}$ *is* good for covering *if*

$$\lim_{n\to\infty} \frac{r_\Lambda^{cov}}{r_\Lambda^{eff}} = 1 \tag{2.8}$$

These lattices are also commonly referred to as *Rogers good*, since it was first shown by Rogers that such lattices exist [19].

Definition 10 (Goodness for quantization)**.** *A sequence of lattices* $\Lambda^{(n)}$ *is* good for quantization *if*

$$\lim_{n\to\infty} G(\Lambda) = \frac{1}{2\pi e} \tag{2.9}$$

In other words, the normalized second moment of Λ approaches to a sphere's normalized second moment as $n \to \infty$. Zamir *et al.*, have shown that such a sequence of lattices exist [11]. Erez *et al.* have also shown the existence of such a sequence of lattices and proved that goodness for covering implies goodness for quantization [8].

Definition 11 (Lattices that achieve the Poltyrev limit)**.** *Let* $\underline{z}$ *be an* n*-dimensional independent and identically distributed (i.i.d) Gaussian vector,* $\underline{z} \sim \mathcal{N}\left(\underline{0}, \theta_{\underline{z}}^2 \mathbf{I}\right)$*. The* effective radius *of* $\underline{z}$*, which we denote as* $r_{\underline{z}}$*, is defined as*

$$r_{\underline{z}} = \sqrt{n\theta_{\underline{z}}^2} \tag{2.10}$$

Consider a $\mathbb{Z}$*-lattice* Λ *and a lattice point* $\underline{\lambda} \in \Lambda$*, which is transmitted across an AWGN channel:*

$$\underline{y} = \underline{\lambda} + \underline{z} \tag{2.11}$$

The maximum likelihood decoder would decode to the lattice point nearest in Euclidean distance to $\underline{y}$*. Therefore, an error would occur only if* $\underline{y}$ *leaves the Voronoi region of* $\underline{\lambda}$*. Due to lattice symmetry, this is equivalent to* $\underline{z}$ *leaving the fundamental Voronoi region* $\mathcal{V}_\Lambda$*.*

$$P_e(\Lambda, r_{\underline{z}}) = Pr\{\underline{z} \notin \mathcal{V}_\Lambda\} \tag{2.12}$$

where $P_e(\Lambda, r_{\underline{z}})$ *denotes the probability of error.*

A sequence of $\mathbb{Z}$*-lattices* $\Lambda^{(n)}$ *are* good for AWGN channel coding *if for any* $r_{\underline{z}} < r_{\Lambda}^{eff}$, $\lim_{n\to\infty} P_e(\Lambda, r_{\underline{z}}) = 0$ *and this decay may be bounded exponentially in* n*. Erez et. al. have shown the existence of such a sequence of lattices in [8] and they have referred to them as* Poltyrev good*. Nonetheless, in order to achieve the Poltyrev capacity in the unconstrained AWGN channel, it is sufficient for* $\lim_{n\to\infty} P_e(\Lambda, r_{\underline{z}}) = 0$ *for any* $r_{\underline{z}} < r_{\Lambda}^{eff}$*, i.e.,* $P_e(\Lambda, r_{\underline{z}})$ *does not need to decay exponentially as* $n \to \infty$*. We refer to such a sequence of lattices as* lattices that achieve the Poltyrev limit *in this dissertation. Loeliger has shown the existence of such lattices in [15].*

Definition 12 (Sublattice)**.** *A* $\mathbb{Z}$*-lattice* Λ *is a sublattice of (nested in) another* $\mathbb{Z}$*-lattice* Λ_f *if* $\Lambda \subseteq \Lambda_f$*.* Λ *is referred to as the* coarse lattice *and* Λ_f *is referred to as the* fine lattice*. The quotient group* Λ_f/Λ *is referred to as a lattice partition [17].*

Definition 13 (Nesting ratio)**.** *Given a pair of* n*-dimensional nested lattices* $\Lambda \subset \Lambda_f$*, the nesting ratio* ϑ *is defined as,*

$$\vartheta = \left(\frac{Vol(\mathcal{V}_\Lambda)}{Vol(\mathcal{V}_{\Lambda_f})} \right)^{\frac{1}{n}}. \tag{2.13}$$

Definition 14 (Nested Lattice Code)**.** *Given a fine* $\mathbb{Z}$*-lattice* Λ_f *and a coarse* $\mathbb{Z}$*-lattice* Λ*, where* $\Lambda \subseteq \Lambda_f$*, a* nested lattice code *(Voronoi code), which we refer to as* $\mathcal{L}$*, is the set of all coset leaders in* Λ_f *that lie in the fundamental Voronoi region of the coarse lattice* Λ *[32]:*

$$\mathcal{L} = \mathcal{V}_\Lambda \cap \Lambda_f = \left\{ \underline{\lambda}_f \ : \ Q_\Lambda\left(\underline{\lambda}_f\right) = \underline{0}, \underline{\lambda}_f \in \Lambda_f \right\}. \tag{2.14}$$

In other words, $\mathcal{L}$ *is a set of coset representatives of the quotient group* Λ_f/Λ*.*

The coding rate of a nested lattice code, denoted as R is defined as,

$$R = \log \vartheta. \tag{2.15}$$

In Fig. 2.4, we depict a nested lattice code. The encircled points are the coarse lattice points and the non-encircled points are the fine lattice points. The nested lattice code would be the points that lie within the Voronoi region of the all-zero coarse lattice point. Note that the nesting ratio would be $\vartheta = \sqrt{7}$.

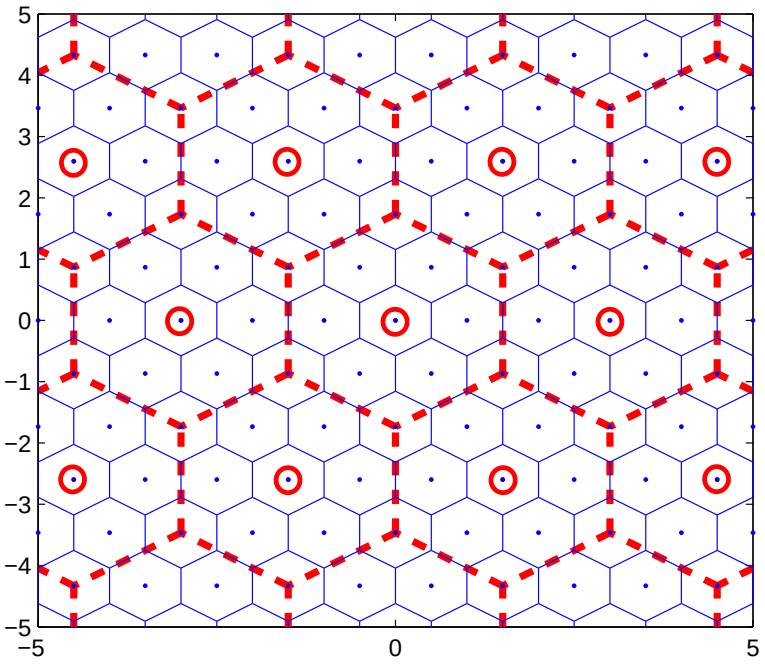

Figure 2.4: Nested lattice code

2.2.1 Construction A for $\mathbb{Z}$-lattices

Throughout the years, various methods have been proposed to construct lattices such as Construction A, Construction B, Construction D, Construction D' [10]. In this dissertation, we will mainly focus on lattices built with Consruction A [33]. Construction A can be described as follows:

Let q be a natural prime and k, n be integers such that $k \leq n$. Then, let $\mathbf{G} \in \mathbb{F}_q^{n \times k}$.

1. Define the discrete codebook $\mathcal{C} = \{\underline{x} = \mathbf{G}\underline{y} : \underline{y} \in \mathbb{F}_q^k\}$ where all operations are over $\mathbb{F}_q$. Thus, $\underline{x} \in \mathbb{F}_q^n$.

2. Generate the $\mathbb{Z}$-lattice $\Lambda_{\mathcal{C}}$ as $\Lambda_{\mathcal{C}} \triangleq \{\underline{\lambda} \in \mathbb{Z}^n : \underline{\lambda} \mod q \in \mathcal{C}\}$, where the mod operation is applied to each component of $\underline{\lambda}$.

3. Scale $\Lambda_{\mathcal{C}}$ with q^{-1} to obtain $\Lambda = q^{-1}\Lambda_{\mathcal{C}}$.

In Fig. 2.5 and Fig. 2.6, a linear code over $\mathbb{F}_{13}$ with a generator matrix $\mathbf{G} = [1\ 4]$ and the resultant lattice built using Construction A is depicted, respectively. As one might observe from these figures, Construction A may be summarized as the tiling of a scaled linear code over $\mathbb{R}^n$. Therefore, many of the underlying linear code's properties will translate to the lattice. We would also like to note that only the first two steps that we have stated in Construction A is required to build a lattice, since the third step simply scales the lattice. However when Erez *et. al.* prove the existence of lattices built with Construction A that are good for covering in [8], they keep r_{Λ}^{eff} approximately constant as $n \to \infty$ and $q \to \infty$, which is possible only if the third step is used for scaling the lattice.

2.2.2 Nested $\mathbb{Z}$-lattices obtained from Construction A [9]

Let Λ be an n-dimensional $\mathbb{Z}$-lattice obtained through Construction-A with a corresponding generator matrix $\mathbf{B}$. For a given $\mathbf{G} \in \mathbb{F}_q^{n \times k}$, denote Λ' as the corre-

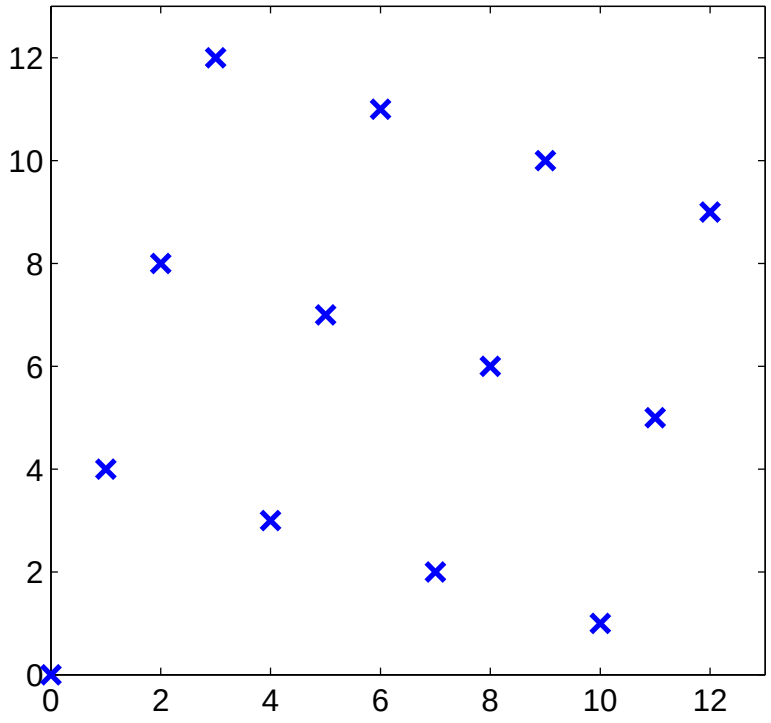

Figure 2.5: Linear code over $\mathbb{F}_{13}$ with $\mathbf{G} = [1\ 4]$

sponding $\mathbb{Z}$-lattice obtained through Construction-A using $\mathbf{G}$ as the generator matrix of the underlying linear code. Generate the $\mathbb{Z}$-lattice Λ_f as $\Lambda_f = \mathbf{B}\Lambda'$. It can be observed that $\Lambda \subset \Lambda_f$ with a coding rate of $\frac{k}{n} \log q$.

Nested lattice codes built using Construction A play a fundamental role in the lattice-based framework proposed in [24] and [6]. This is due to the fact that various properties of lattices that are simultaneously good for AWGN channel coding and good for quantization are required in order to achieve the computation rates stated in [24], [6] and Construction A is the most commonly used method to construct such lattices [8].

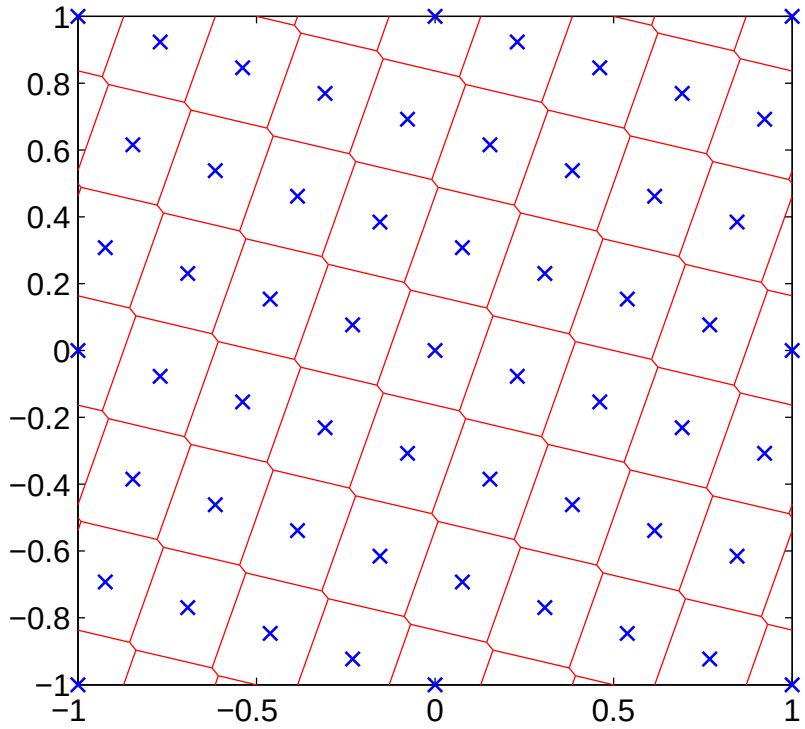

Figure 2.6: Scaled and replicated linear code

2.3 AWGN relay network

In an AWGN relay network, L source nodes $S_1, S_2, \ldots, S_L$ wish to transmit information to M relay nodes $D_1, D_2, \ldots, D_M$, where $M \geq L$. It is assumed that relay nodes can not collaborate with each other and are noiselessly connected to a final destination interested in the individual messages sent from all the source nodes. The objective of the relay nodes is to facilitate communication between the source nodes and the final destination.

We denote the information vector at the source node S_l as $\underline{w}_l \in \mathbb{F}_q^k$. Without loss of generality, we assume that each transmitter l has the same information vector length k. Each transmitter is equipped with an encoder $\mathcal{E}_l : \mathbb{F}_q^k \to \mathbb{C}^n$ that maps $\underline{w}_l$

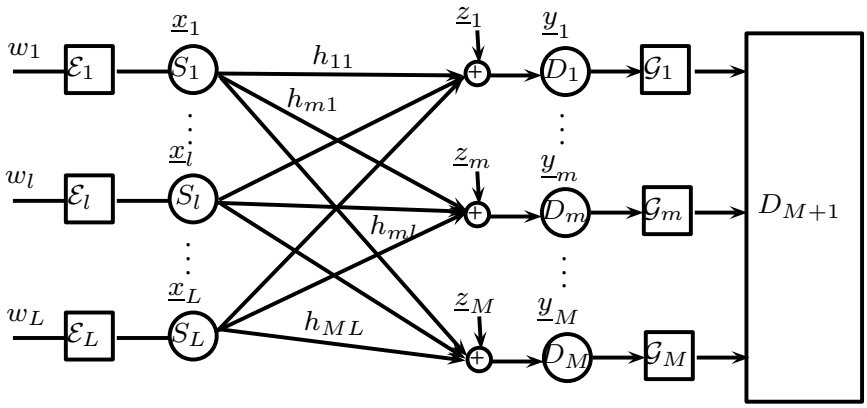

Figure 2.7: AWGN relay network

to an n-dimensional complex codeword $\underline{x}_l = \mathcal{E}_l(\underline{w}_l)$. Each codeword is subject to the power constraint

$$\mathbb{E}||\underline{x}_l||^2 \leq nP. \tag{2.16}$$

The message rate R of each transmitter is the length of its message in bits normalized by the number of channel uses,

$$R = \frac{k}{n} \log q. \tag{2.17}$$

Due to the superposition nature of the wireless medium (assuming perfect synchronization), each relay m observes

$$\underline{y}_m = \sum_{l=1}^{L} h_{ml} \underline{x}_l + \underline{z}_m \tag{2.18}$$

where $h_{ml} \in \mathbb{C}$ is the channel coefficient between D_m and S_l. Furthermore, $\underline{z}_m$ is an n-dimensional complex independent and identically distributed (i.i.d) Gaussian

random variable, i.e. $\underline{z}_m \sim \mathbb{C}\mathcal{N}(0, \mathbf{I})$. Let $\underline{h}_m = [h_{m1}, \cdots, h_{mL}]^T$ denote the vector of channel coefficients to relay m from all the source nodes. We assume that relay m is only required to know the channel coefficient from each transmitter to itself, i.e., $\underline{h}_m$.

Each relay attempts to recover the linear combination $\underline{f}_m$ (over $\mathbb{F}_q$)

$$\underline{f}_m = \bigoplus_{l=1}^{L} (b_{ml} \underline{w}_l) \tag{2.19}$$

where $b_{ml} \in \mathbb{F}_q$ and let $\underline{b}_m = [b_{m1}, \ldots, b_{mL}]^T$. Typically b_{ml}s are chosen based on the network structure and/or the channel coefficients. It is desirable for the matrix $[\underline{b}_1, \ldots, \underline{b}_M]$ to be full-rank which enables each $\underline{w}_l$ to be recovered at the final destination. For each D_m, we define the decoder $\mathcal{G}_m : \mathbb{C}^n \to \mathbb{F}_q^k$, where $\hat{\underline{f}}_m = \mathcal{G}_m(y_m)$ is an estimate of $\underline{f}_m$. The relays then forward $\hat{\underline{f}}_m$'s to a central destination node, denoted as D_{M+1} in Fig. 2.7, which attempts to determine the individual messages w_l.

Definition 15 (Probability of error)**.** *Equations with coefficient vectors $\underline{a}_1, \underline{a}_2, \ldots \underline{a}_m \in \mathbb{Z}[i]^L$ are decoded with probability of error ϵ if*

$$Pr\left(\bigcup_{m=1}^{M} \left\{ \hat{\underline{f}}_m \neq \underline{f}_m \right\} \right) < \epsilon \tag{2.20}$$

Definition 16 (Computation rate of relay m)**.** *For a given channel coefficient vector $\underline{h}_m$ and equation coefficient vector $\underline{a}_m \in \mathbb{Z}^k$, the computation rate $R(\underline{h}_m, \underline{a}_m)$ is achievable at relay m if for any $\epsilon > 0$ and n large enough, there exist encoders $\mathcal{E}_1, \ldots, \mathcal{E}_L$ and there exists a decoder $\mathcal{G}_m$ such that relay m can recover its desired*

equation with probability of error ϵ as long as the underlying message rate R satisfies

$$R < R\left(\underline{h}_m, \underline{a}_m\right). \tag{2.21}$$

Due to the fact that the relays can not collaborate, each relay picks an integer vector $\underline{a}_m$ such that $R\left(\underline{h}_m, \underline{a}_m\right)$ is maximized.

Definition 17 (Computation rate of AWGN network)**.** *Given* $\mathbf{H} = [\underline{h}_1, \ldots, \underline{h}_m]$ *and* $\mathbf{A} = [\underline{a}_1, \ldots, \underline{a}_m]$*, the achievable computation rate of an AWGN network is defined as*

$$\mathcal{R}\left(\mathbf{H}, \mathbf{A}\right) = \min_{m:a_{ml} \neq 0} R\left(\underline{h}_m, \underline{a}_m\right), \tag{2.22}$$

where the corresponding $\mathbf{B} = [\underline{b}_1, \ldots, \underline{b}_M]$ *is full rank. If* $\mathbf{B}$ *is not full rank,* $\mathcal{R}\left(\mathbf{H}, \mathbf{A}\right) = 0$.

2.4 Nazer and Gastpar's lattice-based CF framework

In [6], Nazer and Gastpar use nested lattice codes to implement the compute-and-forward paradigm for the AWGN relay network. Since lattices are closed under integer combinations, the relays attempt to decode to a linear combination of codewords with integer coefficients. This can then be shown to correspond to decoding linear combinations over the finite field. We briefly discuss how lattice codes are constructed to implement the compute-and-forward paradigm in [6].

A fine $\mathbb{Z}$-lattice Λ_f and a coarse $\mathbb{Z}$-lattice Λ nested in Λ_f, is constructed as mentioned in Section 2.2.2 with a coding rate $R = \frac{k}{n} \log q$. If Λ is simultaneously good for covering and good AWGN channel coding, it follows that Λ_f is good for AWGN channel coding [9]. Both Λ and Λ_f are scaled such that $\sigma_\Lambda^2 = P/2$. Following this, the lattice codebook $\Lambda_f \cap \mathcal{V}_\Lambda$ is constructed.

Source node l partitions its information vector $\underline{w}_l \in \mathbb{F}_q^{2k}$ into $\underline{w}_l^R, \underline{w}_l^I \in \mathbb{F}_q^k$, and maps them to lattice codewords $\underline{t}_l^R, \underline{t}_l^I \in \Lambda_f \cap \mathcal{V}$, respectively, via a bijective mapping $\tilde{\psi}$,

$$\tilde{\psi}(\underline{w}) = \left[\mathbf{B}q^{-1}g(\mathbf{G}\underline{w})\right], \tag{2.23}$$

where $\underline{w} \in \mathbb{F}_q^k$, and g is the trivial bijective mapping between $\{0, 1, \cdots, q-1\}$ and $\mathbb{F}_q$. Hence, $\underline{t}_l^R = \tilde{\psi}\left(\underline{w}_l^R\right), \underline{t}_l^I = \tilde{\psi}\left(\underline{w}_l^I\right)$. It then constructs dither vectors $\underline{d}_l^R, \underline{d}_l^I$, which are uniformly distributed within $\mathcal{V}$ and subtracts these dither vectors from the lattice codewords $\underline{t}_l^R, \underline{t}_l^I$, respectively, and transmits the following:

$$\underline{x}_l = \left(\left[\underline{t}_l^R - \underline{d}_l^R\right] \mod \Lambda\right) + j\left(\left[\underline{t}_l^I - \underline{d}_l^I\right] \mod \Lambda\right). \tag{2.24}$$

Recall that given a channel coefficient vector $\underline{h}_m \in \mathbb{C}^L$, relay m observes

$$\underline{y}_m = \sum_{l=1}^{L} h_{ml}\underline{x}_l + \underline{z}_m. \tag{2.25}$$

The relay approximates $\underline{h}_m$, in some sense, by a Gaussian integer vector $\underline{a}_m \in \mathbb{Z}[i]^L$ and its goal will be to recover the following:

$$\underline{v}_m^R = \left[\sum_{l=1}^{L} \Re\left(a_{ml}\right)\underline{t}_l^R - \Im\left(a_{ml}\right)\underline{t}_l^I\right] \mod \Lambda \tag{2.26}$$

$$\underline{v}_m^I = \left[\sum_{l=1}^{L} \Im\left(a_{ml}\right)\underline{t}_l^R + \Re\left(a_{ml}\right)\underline{t}_l^I\right] \mod \Lambda \tag{2.27}$$

It proceeds by removing the dithers and scaling the observation with α_m and there-

fore,

$$\begin{aligned}\underline{\tilde{y}}_m^R &= \Re\left(\alpha_m \underline{y}_m\right) + \sum_{l=1}^{L} \Re\left(a_{ml}\right) \underline{d}_l^R - \Im\left(a_{ml}\right) \underline{d}_l^I \\ &= \underline{v}_m^R + \underline{z}_{eq,m}^R \end{aligned} \tag{2.28}$$

and

$$\begin{aligned}\underline{\tilde{y}}_m^I &= \Im\left(\alpha_m \underline{y}_m\right) + \sum_{l=1}^{L} \Im\left(a_{ml}\right) \underline{d}_l^R + \Re\left(a_{ml}\right) \underline{d}_l^I \\ &= \underline{v}_m^I + \underline{z}_{eq,m}^I \end{aligned} \tag{2.29}$$

where α_m is the MMSE scaling coefficient that minimizes the variance of $\underline{z}_{eq,m}^R + j\underline{z}_{eq,m}^I$. The relay quantizes $\underline{\tilde{y}}_m^I, \underline{\tilde{y}}_m^R$ to the closest lattice points in the fine lattice Λ_f modulo the coarse lattice Λ and estimates the following:

$$\underline{\hat{v}}_m^R = \left[Q\left(\underline{\tilde{y}}_m^R\right)\right] \mod \Lambda \tag{2.30}$$

$$\underline{\hat{v}}_m^I = \left[Q\left(\underline{\tilde{y}}_m^I\right)\right] \mod \Lambda \tag{2.31}$$

where Q denotes the quantization with respect to Λ_f. Finally, the relay maps $\underline{\hat{v}}_m^R$ and $\underline{\hat{v}}_m^I$ to $\underline{\hat{f}}_m^R$ and $\underline{\hat{f}}_m^I$, respectively, via $\tilde{\psi}^{-1}$,

$$\tilde{\psi}^{-1}(\underline{v}) = \left(\mathbf{G}^T\mathbf{G}\right)^{-1}\mathbf{G}^T g^{-1}\left(q\left(\left[\mathbf{B}^{-1}\underline{v} \mod \Lambda\right]\right)\right) \tag{2.32}$$

where $\underline{v} \in \mathbb{F}_q^n$. Hence,

$$\tilde{\psi}^{-1}\left(\hat{\underline{v}}_m^R\right) = \hat{\underline{f}}_m^R = \bigoplus_{l=1}^{L} \left(b_{ml}^R \hat{\underline{w}}_l^R \oplus \left(-b_{ml}^I\right) \hat{\underline{w}}_l^I\right) \tag{2.33}$$

$$\tilde{\psi}^{-1}\left(\hat{\underline{v}}_m^I\right) = \hat{\underline{f}}_m^I = \bigoplus_{l=1}^{L} \left(b_{ml}^I \hat{\underline{w}}_l^R \oplus \left(b_{ml}^R\right) \hat{\underline{w}}_l^I\right) \tag{2.34}$$

where

$$b_{ml}^R = \Re\left(a_{ml}\right) \mod q \tag{2.35}$$

$$b_{ml}^I = \Im\left(a_{ml}\right) \mod q. \tag{2.36}$$

Note that both $[\underline{b}_1^R, \ldots, \underline{b}_M^R]$ and $[\underline{b}_1^I, \ldots, \underline{b}_M^I]$ are required to be full rank so that decoding each $\underline{w}_l^R, \underline{w}_l^I$ at the final destination is feasible.

In [6], Nazer and Gastpar show the following theorem using the coding scheme we have described in this section.

Theorem 18 (Nazer and Gastpar)**.** *At relay m, given $\underline{h}_m \in \mathbb{C}^L$ and $\underline{a}_m \in \mathbb{Z}[i]^L$, a computation rate of*

$$\mathcal{R}(\underline{h}_m, \underline{a}_m) = \log^+\left(\left(\|\underline{a}_m\|^2 - \frac{P|\underline{h}_m^H \underline{a}_m|^2}{1 + P\|\underline{h}_m\|^2}\right)^{-1}\right), \tag{2.37}$$

is achievable.

Given $\mathbf{H}$ and assuming that the relays do not cooperate with each other, each relay would attempt to pick an integer vector $\underline{a}_m$ that maximizes its individual computation rate, i.e. $\underline{a}_m = \arg\max_{\underline{a} \in \mathbb{Z}[i]^L} \mathcal{R}(\underline{h}_m, \underline{a}_m)$ in order to maximize $\mathcal{R}\left(\mathbf{H}, \mathbf{A}\right)$.

3. LATTICES OVER EISENSTEIN INTEGERS FOR CF*

In this chapter, we propose the use of lattice codes over Eisenstein integers for implementing a compute-and-forward protocol in wireless networks when channel state information is not available at the transmitter. We extend the compute-and-forward paradigm of Nazer and Gastpar to decoding Eisenstein integer combinations of transmitted messages at relays by proving the existence of a sequence of nested lattices over Eisenstein integers in which the coarse lattice is good for covering and the fine lattice can achieve the Poltyrev limit. Using this result, we show that the outage performance of nested lattice codebooks over Eisenstein integers surpasses the outage performance of lattice codebooks over integers considered by Nazer and Gastpar with no additional computational complexity. We then propose a separation based compute-and-forward (SBCF) scheme based on the concatenation of a non-binary linear code with a modulation scheme derived from the ring of Eisenstein integers, which can equivalently be thought of as a lattice code which is a subset of a lattice built from Construction A. The SBCF scheme enables the demodulation and decoding to be separated and results in theoretically achievable computation rates that locally surpass Nazer and Gastpar's scheme.

3.1 Introduction

Lattice codes have been shown to be optimal for several problems in communications including coding for the point-to-point additive white Gaussian noise (AWGN) channel and coding with side information problems such as the dirty paper coding problem and Wyner-Ziv problem [9], [29]. The construction of optimal lattice codes

*Reprinted with permission from "Lattices over Eisenstein Integers for Compute-and-Forward" by N. E. Tunali, K. R. Narayanan, J. J. Boutros, and Y. C. Huang, 2012. Proceedings 50th Annual Allerton Conference, pp. 33-40, copyright [2012] by IEEE.

for these problems requires a lattice that is good for channel coding. Since a lattice has unconstrained power, goodness for channel coding is measured using Poltyrev's idea of the unconstrained AWGN channel. In [18], Poltyrev derives the maximum noise variance that a lattice can tolerate while maintaining reliable communication over the unconstrained point-to-point AWGN channel, which is referred to as the Poltyrev limit in literature. Loeliger showed the existence of lattices that achieve the Poltyrev limit by means of Construction A in [15]. Then, Erez *et al.*, showed that there exists lattices which are simultaneously good for quantization and can achieve the Poltyrev limit in [8] which made it possible to construct nested lattice codes that were able to achieve a rate of $\frac{1}{2}\log\left(1+\mathrm{SNR}\right)$ over the point-to-point AWGN channel. There has also been great interest in constructing lattice codes with reasonable encoding and decoding complexities such as Signal Codes and Low Density Lattice Codes [13], [12]. However, one of the main drawbacks of these codes is the computational complexity of their decoding algorithms.

In a bidirectional relay network with unit channel gains, the relay can decode to the sum of the transmitted signals, which is a special case of compute-and-forward. For this system model, it was shown that an exchange rate of $\frac{1}{2}\log\left(\frac{1}{2}+\mathrm{SNR}\right)$ can be achieved using nested lattice codes at the transmitters, which is optimal for asymptotically large signal-to-noise ratios and provides substantial gains over other relaying paradigms such as amplify-and-forward and decode-and-forward [24], [25]. In [37], a novel compute-and-forward implementation is proposed for the $K \times K$ AWGN interference network where channel state information is available at the transmitters, which achieves the full K degrees of freedom.

In this chapter, we consider the case when channel state information is not available at the transmitters. In this case, an effective way to implement a compute-and-forward scheme is to allow the relay to adaptively choose the integer coefficients

depending on the channel coefficients. Nazer and Gastpar have introduced and analyzed such a scheme which uses lattices over integers and they have derived achievable information rates in [6]. In [7], Feng, Silva and Kschischang have introduced an algebraic framework for designing good lattice codes which allow the recovery of linear combinations of transmitted signals over a finite field. They also show that Nazer and Gastpar's scheme in [6] can be seen as a special case of the general framework in [7].

In this chapter, we show that the results in [6] can be extended to lattices over Eisenstein integers and we show that this results in improved outage performance compared to using lattices over integers. We proceed by proving the existence of a sequence of nested lattices over Eisenstein integers in which the coarse lattice is good for covering and the fine lattice achieves the Poltyrev limit. Using this result, we extend the framework in [6] to lattices over Eisenstein integers. The main improvement in outage performance is a result of the fact that the use of lattices over Eisenstein integers permits the relay to decode to a linear combination of the transmitted signals where the coefficients are Eisenstein integers, which quantize channel coefficients better than Gaussian integers. We also propose a separation based compute-and-forward (SBCF) scheme which employs lattice codes constructed from linear codes over a prime-sized field that are mapped to modulation alphabets selected from the ring of Eisenstein integers according to a ring homomorphism. Hence, these lattice codes are essentially obtained from lattices built with Contruction A. However the main difference of the SBCF scheme from the framework in [6] is instead of approximating the channel by an integer integer vector and decoding to the closest point in the lattice, we perform soft-output demodulation based on the channel itself and the chosen function. Therefore, no additional noise from quantizing the channel exists in the SBCF scheme. We then forward the posterior probabilities to a practically imple-

mentable decoder. Through Monte-Carlo simulations, the SBCF scheme is shown to locally achieve higher rates than the coding scheme in [6] extended to Eisenstein integers with practical encoding and decoding complexities. Our proposed scheme also belongs to the general framework introduced by Feng *et. al.*; however, the specific scheme not been analyzed in detail in the literature.

The structure of this chapter is as follows. In Section 3.2, we discuss how lattices over Eisenstein integers can be used for compute-and-forward in Nazer and Gastpar's framework and what properties of these lattices are required in order to achieve computation rates formulated similarly to those in [6]. In Section 3.3, we introduce the SBCF scheme and in Section 3.4, we present simulation results of the SBCF scheme.

3.2 Compute-and-forward with lattices over Eisenstein integers

The main result in this section is that for some channel realizations, higher information rates than those in Theorem 18 are achievable. The improved information rate is obtained by considering nested lattices over Eisenstein integers which allow the mth relay to decode a linear combination of the form $\sum_{l=1}^{L} a_{ml}\underline{t}_l$, where $a_{ml} \in \mathbb{Z}[\omega]$. This result is made precise in Theorem 23.

One of the key challenges in proving this achievability result is to show the existence of nested lattices over Eisenstein integers, which we refer to as $\mathbb{Z}[\omega]$-lattices, where the coarse lattice is good for covering and the fine lattice can achieve the Poltyrev limit. We would like to note that, we do not prove the existence of $\mathbb{Z}[\omega]$-lattices that are good for AWGN channel coding, i.e. the error probability can be bounded exponentially in n, in this chapter. Furthermore, we do not require the coarse lattice in the sequence of nested lattices to be simultaneously good for AWGN channel coding and good for covering. In order to state our main theorem, it suffices

to show the existence of nested $\mathbb{Z}[\omega]$-lattices where the coarse lattice is good for covering and the fine lattice can achieve the Poltyrev limit. A similar result is obtained in [36], where the coarse lattice is chosen to be good only for covering and the fine lattice to be good for AWGN channel coding in order to achieve $\frac{1}{2}\log(1+SNR)$ using lattice codes for the point-to-point AWGN channel.

In what follows, we first provide some preliminaries about Eisenstein integers and summarize Construction A for $\mathbb{Z}[\omega]$-lattices. Afterwards, we show that nested $\mathbb{Z}[\omega]$-lattices where the coarse lattice is good for quantization and the fine lattice achieves the Poltyrev limit can be obtained through Construction A. The existence result can then be used to prove Theorem 23, which is the main result of this chapter. Since $\mathbb{Z}[\omega]$ quantizes $\mathbb{C}$ better than $\mathbb{Z}[i]$, on the average (over the channel realizations), higher information rates are achievable by using $\mathbb{Z}[\omega]$-lattices compared to using $\mathbb{Z}$-lattices. In Section 3.2.4, we provide numerical results in order to compare the performance of lattices over natural integers and lattices over Eisenstein integers in compute-and-forward.

3.2.1 Preliminaries: Eisenstein integers

An Eisenstein integer is a complex number of the form $a+b\omega$ where $a,b\in\mathbb{Z}$ and $\omega=-\frac{1}{2}+j\frac{\sqrt{3}}{2}$. The ring of Eisenstein integers $\mathbb{Z}[\omega]$ is a principal ideal domain, i.e, a commutative ring without zero divisors where every ideal can be generated by a single element. Other well-known principal ideal domains are $\mathbb{Z}$ and $\mathbb{Z}[i]$. A *unit* in $\mathbb{Z}[\omega]$ is one of the following:$\{\pm 1,\pm\omega,\pm\omega^2\}$. An Eisenstein integer ϱ is an Eisenstein prime if either one of the following mutually exclusive conditions hold [16]:

1. ϱ is equal to the product of a unit and any natural prime congruent to 2 mod 3.

2. $|\varrho|^2=3$ or $|\varrho|^2$ is any natural prime congruent to 1 mod 3.

An n-dimensional $\mathbb{Z}[\omega]$-lattice can be written in terms of a complex lattice generator matrix $\mathbf{B} \in \mathbb{C}^{n\times k}$:

$$\Lambda = \{\underline{\lambda} = \mathbf{B}\underline{e} : \underline{e} \in \mathbb{Z}[\omega]^k\} \tag{3.1}$$

3.2.2 Construction A for $\mathbb{Z}[\omega]$-lattices

Let ϱ be an Eisenstein prime with $|\varrho|^2 = q$. Then $\varrho\mathbb{Z}[\omega]$ is a sublattice of $\mathbb{Z}[\omega]$ and together, they form the quotient ring $\mathbb{Z}[\omega]/\varrho\mathbb{Z}[\omega]$. Note that the quotient ring has a finite order of $|\mathbb{Z}[\omega]/\varrho\mathbb{Z}[\omega]| = \mathrm{Vol}\left(\mathcal{V}_{\varrho\mathbb{Z}[\omega]}\right)/\mathrm{Vol}\left(\mathcal{V}_{\mathbb{Z}[\omega]}\right) = |\varrho|^2 = q$ and $\mathbb{Z}[\omega]$ is the union of q cosets of $\varrho\mathbb{Z}[\omega]$

$$\mathbb{Z}[\omega] = \bigcup_{s\in\mathcal{S}} (\varrho\mathbb{Z}[\omega] + s) \tag{3.2}$$

where $\mathcal{S}$ represents the set of q coset leaders of $\varrho\mathbb{Z}[\omega]$ in $\mathbb{Z}[\omega]$. Note that one can define a canonical homomorphism $\mod \varrho\Lambda : \mathbb{Z}[\omega] \to \mathbb{Z}[\omega]/\varrho\mathbb{Z}[\omega]$ and a ring isomorphism $\sigma : \mathbb{Z}[\omega]/\varrho\mathbb{Z}[\omega] \leftrightarrow \mathbb{F}_q$. Composing $\mod \varrho\Lambda$ and σ, one can obtain the ring homomorphism $\tilde{\sigma} \triangleq \sigma \circ \mod \varrho\Lambda : \mathbb{Z}[\omega] \to \mathbb{F}_q$ [34, page 118]. Note that $\tilde{\sigma}$ can be extended to vectors in a straightforward manner by mapping the elements of the vector componentwise to another vector [10, page 197]. We can now define Construction A for $\mathbb{Z}[\omega]$-lattices.

Let ϱ be an Eisenstein prime and $q = |\varrho|^2$. Note that q is either a natural prime or the square of a natural prime. Also let k, n be integers such that $k \leq n$ and let $\mathbf{G} \in \mathbb{F}_q^{n\times k}$. Similar to a $\mathbb{Z}$-lattice, a $\mathbb{Z}[\omega]$-lattice can be obtained by Construction A [10].

1. Define the discrete codebook $\mathcal{C} = \{\underline{x} = \mathbf{G}\underline{y} : \underline{y} \in \mathbb{F}_q^k\}$ where all operations are over $\mathbb{F}_q$. Thus, $\underline{x} \in \mathbb{F}_q^n$.

2. Generate the n-dimensional $\mathbb{Z}[\omega]$-lattice $\Lambda_{\mathcal{C}}$ as $\Lambda_{\mathcal{C}} \triangleq \{\lambda \in \mathbb{Z}[\omega]^n : \tilde{\sigma}(\lambda) \in \mathcal{C}\}$.

3. Scale $\Lambda_{\mathcal{C}}$ with ϱ^{-1} to obtain $\Lambda = \varrho^{-1}\Lambda_{\mathcal{C}}$.

Once again, we would like to note that only the first two steps that we have stated in Construction A is required to build a $\mathbb{Z}[\omega]$-lattice. However due to the fact that we will prove the existence of $\mathbb{Z}[\omega]$-lattices that are good for covering in this chapter using similar proof techniques in [8], we also require the third step which scales the lattice. An example of such a construction with $k = 1, n = 1, \mathbf{G} = [1]$, $\varrho = 2 - \sqrt{3}j$ and $q = 7$ is shown in Fig. 3.1 and Fig. 3.2. The labeling of points in $\Lambda_{\mathcal{C}}$ with elements from $\mathbb{F}_7$ is also shown in Fig. 3.2. It can be verified that this labeling, i.e., $\tilde{\sigma}$ is indeed a ring homomorphism. Note that the $\mod q$ operation in Construction A for $\mathbb{Z}$-lattices also provides a ring homomorphism. We would like to note that the lattice in Fig. 3.1 is trivially $\mathbb{Z}[\omega]$, or in other words the A_2 lattice, and the lattice in Fig. 3.2 is a scaled A_2 lattice. Unfortunately, we were not able to provide a less trivial figure with a larger dimensional $\mathbb{Z}[\omega]$-lattice. This is due to the fact that even a two-dimensional $\mathbb{Z}[\omega]$-lattice requires four real dimensions to be drawn, which is not feasible.

Given n, k, q, we define an $(n, k, q, \mathbb{Z}[\omega])$ ensemble as the set of $\mathbb{Z}[\omega]$-lattices obtained through Construction-A where for each of these lattices, $\mathbf{G}_{ij}$ are i.i.d with a uniform distribution over $\mathbb{F}_q$.

Theorem 19. *A lattice Λ drawn from an $(n, k, q, \mathbb{Z}[\omega])$ ensemble, where $k < n$ but grows faster than $\log^2 n$, q is a natural prime congruent to $1 \mod 3$, and where k, q*

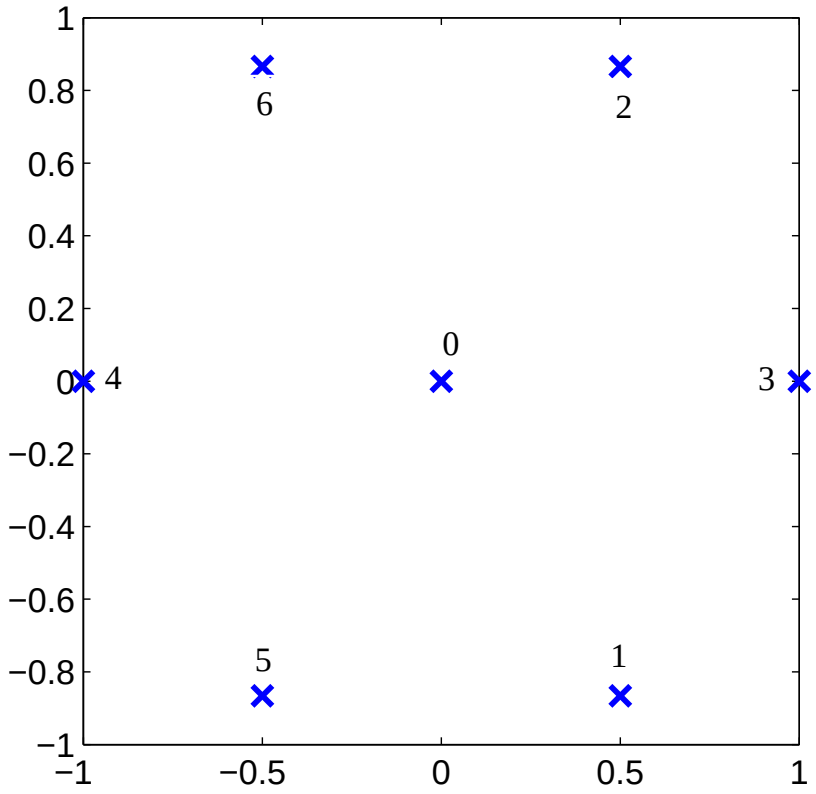

Figure 3.1: $\Lambda_{\mathcal{C}}$ with $\mathbf{G} = [1]$ and the corresponding ring homomorphism

satisfy

$$q^k = \frac{\left(\frac{\sqrt{3}}{2}\right)^n}{V_{\mathcal{B}}\left(r_\Lambda^{eff}\right)} = \frac{\left(\frac{\sqrt{3}}{2}\right)^n \Gamma\left(n+1\right)}{\pi^n \left(r_\Lambda^{eff}\right)^{2n}}$$
$$\approx \sqrt{2n\pi}\left(\frac{\sqrt{3}}{2}\right)^n \left(\frac{2n}{2\exp(1)\left(r_\Lambda^{eff}\right)^2}\right)^n \tag{3.3}$$

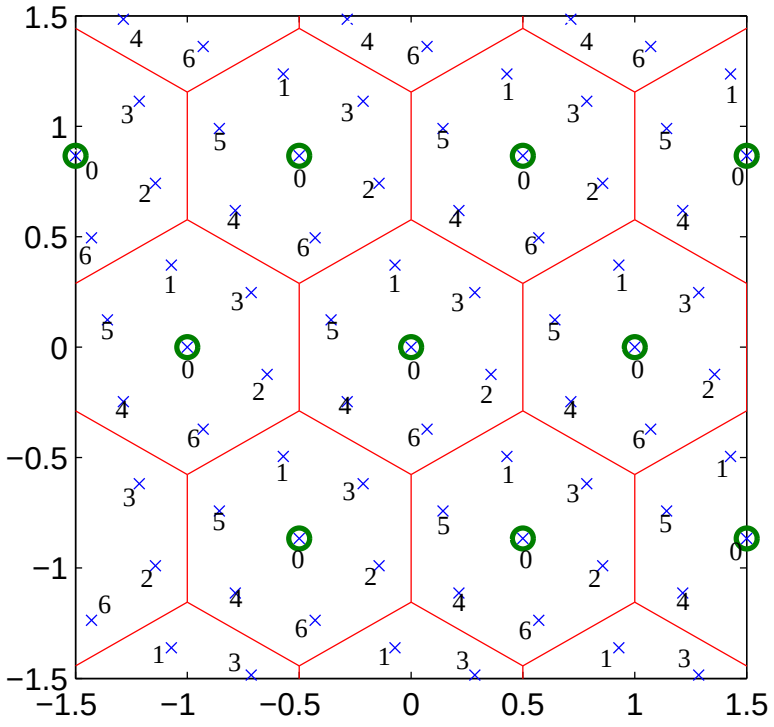

Figure 3.2: $\varrho^{-1}\Lambda_{\mathcal{C}}$ with $\mathbf{G} = [1]$, $\varrho = 2 - j\sqrt{3}$ and the ring homomorphism

and

$$r_{min} < r_{\Lambda}^{eff} < 2r_{min} \tag{3.4}$$

where $0 < r_{min} < \frac{1}{4}$, *is good for covering, i.e,*

$$\frac{r_{\Lambda^{cov}}}{r_{\Lambda}^{eff}} \to 1 \tag{3.5}$$

in probability as $n \to \infty$.

Proof. We first give some definitions and preliminaries that will be very useful for this proof. In [10, p. 54], it is stated that an n-dimensional complex lattice can be

equivalently thought of as a $2n$-dimensional real lattice by the following mapping

$$[\lambda(1)\cdots\lambda(n)]^T \rightarrow [\Re(\lambda(1))\ \Im(\lambda(1))\cdots\Re(\lambda(n))\ \Im(\lambda(n))]^T \tag{3.6}$$

where the left hand side is an n-dimensional complex lattice point and the right hand side is its $2n$-dimensional real representation. Thus we shall consider n-dimensional Eisentein lattices as $2n$-dimensional real lattices and use $\mathbb{C}^n$ and $\mathbb{R}^{2n}$ interchangeably. We shall now introduce the notation that will be used in this section.

- $\mathcal{V}$: Fundamental Voronoi region of the lattice $\mathbb{Z}[\omega]^n$.
- GRID: The lattice $\varrho^{-1}\mathbb{Z}[\omega]^n$, where ϱ is an Eisenstein prime.
- $\underline{x}^* = \underline{x} \mod \mathcal{V} = \underline{x} \mod \mathbb{Z}[\omega]^n = \underline{x} - Q_{\mathbb{Z}[\omega]^n}(\underline{x})$ where $\underline{x} \in \mathbb{C}^n$.
- $\mathcal{A}^* = \mathcal{A} \mod \mathcal{V}$, where $\mathcal{A}$ is any set in $\mathbb{C}^n$ and the $\mod \mathcal{V}$ operation is done element-wise.
- $\mathcal{A}' \triangleq \mathcal{A} \setminus \{0\}$ where $\mathcal{A} \subset \mathbb{R}^n$, $\mathcal{A} \subset \mathbb{C}^n$ or $\mathcal{A} \subset \mathbb{F}_q^n$
- Λ: An n-dimensional $\mathbb{Z}[\omega]$-lattice nested in GRID, i.e., $\Lambda \subset$ GRID .
- Vol$(\cdot)$: Volume of a closed set in $\mathbb{C}^n$, or equivalently volume of a closed set in $\mathbb{R}^{2n}$.
- GRID*: GRID $\cap\, \mathcal{V}$
- $\mathcal{B}(r)$:A complex n-dimensional, or equivalently real $2n$-dimensional, closed set of points inside a sphere of radius r centered at the origin.

- Λ^*: The lattice constellation, i.e. $\Lambda^* = \Lambda \cap \mathcal{V}$. Note that Λ^* can generate Λ as follows:

$$\Lambda = \Lambda^* + \mathbb{Z}[\omega]^n \tag{3.7}$$

- $M = |\Lambda^*|$: Cardinality of the lattice constellation.
- Λ_i^*: A point in Λ^*, $i \in \{0, \cdots, M-1\}$.

Note that by our construction, the lattices chosen from the $(n, k, q, \mathbb{Z}[\omega])$-lattice ensemble are periodic modulo the region $\mathcal{V}$. Thus we can restate all the properties of our lattice in terms of the lattice constellation Λ^* that lies within $\mathcal{V}$. The $(n, k, q, \mathbb{Z}[\omega])$-lattice ensemble has the following properties:

1. $\Lambda_0^* = \underline{0}$ deterministically.

   Proof. $\underline{0}$ is always a valid lattice point due to the definition of a lattice and $\underline{0}^* = \underline{0}$. Thus the result holds. □

2. Λ_i^* is distributed uniformly over GRID^* for $i \in \{1, \cdots, M-1\}$ where $M = q^k$.

   Proof. Each element of $\mathbf{G}$ is chosen uniformly over $\mathbb{F}_q$, therefore each codeword of the underlying linear code is distributed uniformly over $\mathbb{F}_q^n$. Due to last step in Construction A in Section 3.2.2 where the lattice is scaled with ϱ^{-1} and the ring homomorphism $\tilde{\sigma}$, the result holds. □

3. The difference $(\Lambda_i^* - \Lambda_l^*)^*$ is uniformly distributed over GRID^* for all $i \neq j$.

   Proof. This result holds due to the previous property and the definition of the $*$ operation. □

4. $|\Lambda^*| = q^k$ with high probability if $n - k \to \infty$

Proof.

$$\begin{aligned}\Pr\{\text{rank}(\mathbf{G}) < k\} &\leq \sum_{\underline{c} \neq \underline{0}} \Pr\left\{\sum_{i=1}^{k} c_i \mathbf{G}_i = \underline{0}\right\} \\ &= q^{-n}(q^k - 1) \end{aligned} \tag{3.8}$$

where c_i would be elements of a $k \times 1$ coefficient vector $\underline{c}$. □

We shall refer to $\mathcal{B}(r)^* = \mathcal{B}(r) \mod \mathcal{V}$ as a $\mathcal{V}$-ball. Under the assumption that $r < \frac{1}{2}$, we say that $(\Lambda^* + \mathcal{B}(r))^*$ is a $\mathcal{V}$-covering if

$$\mathcal{V} \subseteq \bigcup_{\underline{\lambda} \in \Lambda^*} (\underline{\lambda} + \mathcal{B}(r))^* . \tag{3.9}$$

Note that $\Lambda + \mathcal{B}(r)$ is a covering if and only if $(\Lambda^* + \mathcal{B}(r))^*$is a $\mathcal{V}$-covering

In our lattice ensemble, we will constrain $k < \beta n$ for some $0 < \beta < 1$. Therefore $\Pr\{\text{rank}(\mathbf{G}) \neq k\}$ goes to zero at least exponentially. If $\mathbf{G}$ is full rank, there are $M = q^k$ many codewords that lie in $\mathcal{V}$. Also, an n-dimensional $\mathcal{V}$ is known to have a volume of $\left(\frac{\sqrt{3}}{2}\right)^n$. Then the volume of the Voronoi region of our lattice is equal to $\left(\frac{\sqrt{3}}{2}\right)^n q^{-k}$. In our analysis very similar to [8], we will hold the effective radius of the Voronoi region of Λ, denoted as r_Λ^{eff} approximately constant as $n \to \infty$. This implies

the following:

$$q^k = \frac{\left(\frac{\sqrt{3}}{2}\right)^n}{V_{\mathcal{B}}\left(r_\Lambda^{\text{eff}}\right)} = \frac{\left(\frac{\sqrt{3}}{2}\right)^n \Gamma\left(n+1\right)}{\pi^n \left(r_\Lambda^{\text{eff}}\right)^{2n}}$$
$$= \sqrt{2n\pi}\left(\frac{\sqrt{3}}{2\left(r_\Lambda^{\text{eff}}\right)^2}\right)^n \left(\frac{n}{e}\right)^n \left(1 + O\left(\frac{1}{n}\right)\right) \tag{3.10}$$

Note that q can either be a natural prime congruent to 1 mod 3 or the square of a natural prime congruent to 2 mod 3, nonetheless we shall restrict q to be a natural prime congruent to 1 mod 3 for the sake of simplicity. We would like to note that it is not possible to keep r_Λ^{eff} constant as n grows since q has to be a natural prime congruent to 1 mod 3 and k has to be an integer. Therefore, we will relax this condition to

$$r_{min} < r_\Lambda^{\text{eff}} < 2r_{min} \tag{3.11}$$

as n grows, where $0 < r_{min} < \frac{1}{4}$. Although we have restricted q to be a natural prime congruent to 1 mod 3 , with the assumption of $k \leq \beta n$ for $\beta < 1$, (3.11) can be satisfied for any large enough n due to the following. Let q^* be the real number that satisfies (3.10) for a radius of $2r_{min}$. Then, $q^{*^k} = \frac{1}{V_{\mathcal{B}}(\sqrt{\frac{2}{\sqrt{3}}}2r_{min})}$ and from (3.11), q must satisfy

$$q^* < q < 2^{2n/k} q^*. \tag{3.12}$$

Finally, to show that for each $n > 4$ in our sequence a corresponding q exists that satisfies (3.12), we use the following lemma.

Lemma 20 ([14])**.** *There always exists a natural prime congruent to* 1 mod 3 *be-*

tween integers m and $2m$ where $m > 4$.

We would also like to note that from (3.10), the growth of q is $O(n^{\frac{1}{\beta}})$. Thus,

$$\lim_{n\to\infty} \quad n/q = 0 \tag{3.13}$$

The proof of this theorem is divided into two parts. In the first part, sufficient conditions are obtained such that most Eisenstein lattices in the ensemble are "almost complete" $\mathcal{V}$-coverings. In the second part, stricter conditions are imposed such that most of the Eisentein lattices in the ensemble are *complete* $\mathcal{V}$-coverings and thus *complete* coverings .

Part I: Almost complete covering

Denote d to be half of the largest distance between any two points that lie within the Voronoi region of an element in GRID.

$$d = \sqrt{\frac{n}{3q}} \tag{3.14}$$

Note that by (3.12), $d \to 0$ as $n \to \infty$.

Consider the lattice constellation Λ^* of the ensemble and define k_1, k_2 such that $k_1 + k_2 = k$. We shall denote the Eisenstein lattice constellation obtained from the first k_1 columns of $\mathbf{G}$ by $\Lambda^*[k_1]$ and let $\Lambda^*[k_1 + j], j = 1, \cdots, k_2$ denote the Eisenstein lattice constellation obtained from the first $k_1 + j$ columns of $\mathbf{G}$. Let $\underline{x}$ be an arbitrary point such that $\underline{x} \in \mathcal{V}$. Let $\mathcal{S}_1(\underline{x})$ denote the set of GRID points within a modulo distance $r - d$ from $\underline{x}$ where d was defined in (3.14).

$$\mathcal{S}_1(\underline{x}) = \text{GRID}^* \cap (\underline{x} + \mathcal{B}(r - d))^* \tag{3.15}$$

Furthermore, denote $\mathcal{S}_2(\underline{x})$ to be the set of GRID points such that their Voronoi regions intersect a sphere of radius $r-2d$ centered at $\underline{x}$.

$$\mathcal{S}_2(\underline{x}) = \left\{\underline{y} \in \text{GRID}^* : \left(\underline{y} + \varrho^{-1}\mathcal{V}\right) \cap \left(\underline{x} + \mathcal{B}(r-2d)\right)^*\right\} \tag{3.16}$$

It can be observed that $\mathcal{S}_2(\underline{x}) \subset \mathcal{S}_1(\underline{x})$. Thus, the cardinality of $\mathcal{S}_1(\underline{x})$ can be bounded as:

$$\begin{aligned} |\mathcal{S}_1(\underline{x})| \geq |\mathcal{S}_2(\underline{x})| &\geq \left\lceil V_{\mathcal{B}}(r-2d)/\text{Vol}(\varrho^{-1}\mathcal{V})\right\rceil \\ &= \left\lceil q^n(\sqrt{3}/2)^{-n}V_{\mathcal{B}}(r-2d)\right\rceil \end{aligned} \tag{3.17}$$

By the second property of the ensemble, the probability that $\underline{x}$ is covered by a sphere of radius $(r-d)$ centered at any point of $\Lambda^*[k_1]$ satisfies

$$\begin{aligned} \Pr\left\{\underline{x} \in \left(\Lambda_i^*[k_1] + \mathcal{B}(r-d)\right)^*\right\} = \\ |\mathcal{S}_1(\underline{x})|/q^n \geq (\sqrt{3}/2)^{-n}V_{\mathcal{B}}(r-2d) \end{aligned} \tag{3.18}$$

for $i = 1, \cdots, M_1 - 1$ where $M_1 = q^{k_1}$ and Λ_i^* is the ith point of Λ^*. The indicator random variable η_i for $i = 1, \cdots, M_1 - 1$ is defined as

$$\eta_i = \eta_i(\underline{x}) \begin{cases} 1, & \text{if } \underline{x} \in \left(\Lambda_i^*[k_1] + \mathcal{B}(r-d)\right)^* \\ 0, & \text{otherwise} \end{cases}$$

Note that $i = 0$ is not considered since $\Lambda_0^*[k_1] = 0$ deterministically. Thus, η_i is

statistically independent of both i and $\underline{x}$. Define $\mathcal{X} = \mathcal{X}(\underline{x})$ as follows:

$$\mathcal{X} = \sum_{i=1}^{M_1-1} \eta_i \tag{3.19}$$

Hence, $\mathcal{X}$ is equal to the number of nonzero codewords $(r-d)$-covering $\underline{x}$. Computing the expectation of $\mathcal{X}$ and using the lower bound from (3.18),

$$\begin{aligned} E(\mathcal{X}) &= \sum_{i=1}^{M_1-1} E(\eta_i) \\ &\geq (M_1 - 1)\,(\sqrt{3}/2)^{-n} V_{\mathcal{B}}(r-2d) \end{aligned} \tag{3.20}$$

Since the η_i's are pairwise independent and thus uncorrelated, similar to [8] one has

$$\mathrm{Var}(\mathcal{X}) \leq E(\mathcal{X}) \tag{3.21}$$

Using (3.21), by Chebyshev's inequality, for any $\nu > 0$

$$\Pr\left\{|\mathcal{X} - E(\mathcal{X})| > 2^{\nu}\sqrt{E(\mathcal{X})}\right\} < \frac{\mathrm{Var}(\mathcal{X})}{2^{2\nu}E(\mathcal{X})} \leq 2^{-2\nu} \tag{3.22}$$

Define

$$\mu(\nu) = E(\mathcal{X}) - 2^{\nu}\sqrt{E(\mathcal{X})} \tag{3.23}$$

Then from (3.22),

$$\Pr\{\mathcal{X} < \mu(\nu)\} < 2^{-2\nu} \tag{3.24}$$

If $\mu(\nu) \geq 1$, $\Pr\{\mathcal{X} < 1\}$ is upper-bounded by $2^{-2\nu}$ as well.

A point $\underline{x} \in \mathcal{V}$ will be referred as *remote* from a discrete set of points $\mathcal{A}$ if it is not $r-d$-covered by $(\mathcal{A} + \mathcal{B}(r-d))^*$, i.e. if $\underline{x}$ does not belong to an $(r-d)$- sphere

centered at any point of $\mathcal{A}$. Therefore, $\mathcal{X}(\underline{x}) < 1$ implies that "$\underline{x}$ is remote from $\Lambda^*[k_1]$". Define $\mathcal{Q}(\mathcal{A})$ to be the set of (continuous) points which are remote from the discrete set $\mathcal{A}$. Denote $\mathcal{Q}_i = \mathcal{Q}(\Lambda^*[k_1 + i]), i = 0, 1, \cdots, k_2$ and define

$$q_i = |\mathcal{Q}_i|/\mathrm{Vol}(\mathcal{V}) \tag{3.25}$$

to be the fraction of (continuous) points in $\mathcal{V}$ which are remote from $\Lambda^*[k_1+i]$. Then,

$$|\mathcal{Q}_0| = \int_{\mathcal{V}} \mathbf{1}(\mathcal{X}(\underline{x}) < 1)\, d\underline{x} \tag{3.26}$$

$$\leq \int_{\mathcal{V}} \mathbf{1}(\mathcal{X}(\underline{x}) < \mu(\nu))\, d\underline{x} \tag{3.27}$$

under the condition that $\mu(\nu) > 1$. Then, from (3.24) we have

$$E(q_0) < 2^{-2\nu}. \tag{3.28}$$

Applying Markov's inequality we get

$$\Pr\{q_0 > 2^{\nu} E(q_0)\} < 2^{-\nu}. \tag{3.29}$$

Using (3.28),

$$\Pr\{q_0 > 2^{-\nu}\} < 2^{-\nu}. \tag{3.30}$$

Therefore, by taking $\nu \to \infty$ and keeping $\mu(\nu) \geq 1$, this probability can be made arbitrarily small as $n \to \infty$. In order to satisfy these constraints it is sufficient to take $\nu = o(\log n)$ and $E(\mathcal{X}) > n^{\lambda}$ for some $\lambda > 0$. By (3.20) this would be satisfied

if we choose a radius r such that

$$q^{k_1} - 1 = \frac{n^{\lambda}}{V_{\mathcal{B}}(r-2d)} \left(\sqrt{3}/2\right)^n. \tag{3.31}$$

Hence, we conclude that for these choice of parameters, for most lattices chosen from the $(n, k, q, \mathbb{Z}[\omega])$ ensemble, *almost all* points are covered by spheres of radius $r - d$.

Part II: Complete covering

We would like to obtain an ensemble of $\mathbb{Z}[\omega]$-lattices such that most of its members are able to cover all the points in $\mathcal{V}$. $\mathcal{Q}(\mathcal{A})$ is redefined to be the set of GRID* points, i.e., $\underline{x} \in$ GRID* which are remote from $\mathcal{A}$ and q_i is redefined to be the fraction of GRID* points that are remote from $\Lambda^*[k_1 + i]$. Therefore, an $(r-d)$-covering of all GRID points implies an r-covering of all points in $\mathcal{V}$.

By augmenting the generator matrix $\mathbf{G}$ with an additional small number of columns $k_2 (k_2 \ll k_1)$, the fraction of uncovered GRID* points can be made smaller than $1/|$ GRID$^*|$ which implies that all GRID points are $r-d$-covered. We proceed as follows.

Choose k_1 and q such that k_1 grows faster than $\log^2 n$ and (3.10) and (3.11) are satisfied. Define the set

$$\mathcal{S} = \Lambda^*[k_1] \cup \left(\Lambda^*[k_1] + \left\{\sigma^{-1}(\mathbf{G}_{k_1+1}) \cap \mathcal{V}\right\}\right) \tag{3.32}$$

where σ is the ring isomorphism defined in section 3.2.2. Also note that,

$$\Lambda^*[k_1 + 1] = \bigcup_{m=0}^{q-1} \left(\Lambda^*[k_1] + \sigma^{-1}\left([m \cdot (\mathbf{G}_{k_1+1})] \mod q\right)\right) \tag{3.33}$$

Hence, $\mathcal{S} \subset \Lambda^*[k_1+1]$ and q_1 is upper-bounded by $\frac{\mathcal{Q}(\mathcal{S})}{|\text{GRID}|^*}$. Since $\Lambda^*[k_1]+\{\sigma^{-1}(\mathbf{G}_{k_1+1}) \cap \mathcal{V}\}$ is an independent shift of $\Lambda^*[k_1]$, conditioned on $\Lambda^*[k_1]$, the event that $\underline{x}$ is remote from $\Lambda^*[k_1]+\{\sigma^{-1}(\mathbf{G}_{k_1+1}) \cap \mathcal{V}\}$ is independent from whether $\underline{x}$ is remote from $\Lambda^*[k_1]$ and the probability of such an event is q_0. Then,

$$E\left\{\frac{|\mathcal{Q}(\mathcal{S})|}{|\text{GRID}^*|}\Big|q_0\right\} = q_0^2 \tag{3.34}$$

Due to the fact that $\mathcal{S} \subset \Lambda^*[k_1+1]$, we have $E\{q_1|q_0\} \leq q_0^2$. By Markov's inequality,

$$\Pr\Big\{q_1 > 2^{\gamma} E(q_1|q_0)\Big|q_0\Big\} \tag{3.35}$$

Therefore,

$$\Pr\Big\{q_1 \leq 2^{\gamma-2\nu}\Big|q_0 \leq 2^{-\nu}\Big\} \geq 1-2^{-\gamma} \tag{3.36}$$

From Bayes' rule and (3.30),

$$\Pr\Big\{q_1 \leq 2^{\gamma-2\nu}\Big\} \geq \Pr\Big\{q_1 < 2^{\gamma-2\nu}, q_0 \leq 2^{-\nu}\Big\} \tag{3.37}$$

$$\geq \left(1-2^{-\gamma}\right)\left(1-2^{-\nu}\right) \tag{3.38}$$

Repeating this procedure for $l = 0, 1, \ldots, k_2-1$, we obtain

$$q_{l+1} \leq 2^{\gamma} E(q_{l+1}|q_l) \tag{3.39}$$

$$\leq 2^{\gamma} q_l^2 \tag{3.40}$$

with probability at least $1-2^{-\gamma}$. Hence, the intersection of all these k_2 events and

the event that $q_0 < 2^{-\nu}$ has the probability $(1-2^{-\nu})\,(1-2^{-\gamma})^{k_2}$, which implies

$$q_{k_2} \leq 2^{2^{k_2}(\gamma-\nu)-\gamma} \tag{3.41}$$

We would like to choose k_2 such that

$$q_{k_2} < q^{-n} = 2^{-n\log q}. \tag{3.42}$$

The interpretation of (3.42) is $q_{k_2} = 0$ since there are q^n points in GRID*. Therefore, choosing $\gamma = \nu - 1$ and

$$k_2 = \lceil \log n + \log\log q \rceil \tag{3.43}$$

or faster suffices. Due to the fact that $k = k_1 + k_2$, we conclude that with probability at least

$$\left(1-2^{-\nu}\right)\left(1-2^{-\nu+1}\right)^{(\log n+\log\log q)} \tag{3.44}$$

$\Lambda^*[k]$ satisfies $q_{k_2} < q^{-n}$, in other words every $\underline{x} \in \text{GRID}^*$ is covered by at least one sphere of radius $(r-d)$. We would like to impose a condition on ν such that both $\nu \to \infty$ and the probability in (3.44) goes to 1 as $n \to \infty$. It suffices to choose

$$\nu = 2\log\left(\log n + \log\log q\right). \tag{3.45}$$

Note that as $\mu(\nu) \geq 1$, the probability that there remains a point $\underline{x} \in \text{GRID}^*$ that is not $(r-d)$-covered is arbitrarily small as $n \to \infty$. If every point of GRID* is $(r-d)$-covered, then $\mathcal{V}$ is r-covered. Thus, the probability of a complete covering

with spheres of radius r goes to 1 where r satisfies(see (3.31))

$$M = q^{k_1+k_2} = \frac{n^\lambda}{V_{\mathcal{B}}(r-2d)} \left(\sqrt{3}/2\right)^n q^{k_2} \tag{3.46}$$

$$\leq \frac{n^\lambda}{V_{\mathcal{B}}(r-2d)} \left(\sqrt{3}/2\right)^n q^{(\log n + \log\log q)+1} \tag{3.47}$$

$$= \frac{n^\lambda}{V_{\mathcal{B}}(r-2d)} \left(\sqrt{3}/2\right)^n 2^{\log q[(\log n + \log\log q)+1]} \tag{3.48}$$

From (3.46) and (3.48),

$$\frac{r}{r_\Lambda^{\text{eff}}} = \sqrt[2n]{\frac{V_{\mathcal{B}}(r)}{V_{\mathcal{B}}(r-2d)} n^\lambda q^{k_2}} \tag{3.49}$$

$$\leq \left(\frac{r}{r-2d}\right) \cdot n^{\lambda/2n} \cdot 2^{(\log q \log n + \log q \log\log q + \log q)/2n} \tag{3.50}$$

For $\rho_{\text{cov}} \to 1$, the left-hand side of (3.49) should go to 1. Hence, we require each of the three terms on the right-hand side of (3.50) goes to 1. From (3.13) and (3.14), it follows that $d \to 0$ as $n \to \infty$ provided that $k \leq \beta n$ and $\beta < 1$. Therefore,

$$\lim_{n\to\infty} \left(\frac{r}{r-2d}\right) = 1 \tag{3.51}$$

For any fixed $\lambda > 0$, we have $\lim_{n\to\infty} n^{\lambda/2n} = 1$. Also, since k grows faster than $\log^2 n$, by (3.10) we have $\log p$ grows slower than $o\log(n/\log n)$. Then,

$$\lim_{n\to\infty} 2^{(\log q \log n + \log q \log\log q + \log q)/2n} = 1 \tag{3.52}$$

Thus, we have that $\frac{r_\Lambda^{\text{cov}}}{r_\Lambda^{\text{eff}}} \to 1$ in probability as $n \to \infty$ which completes the proof.

□

We would like to note that a variant of Theorem 19 can also be proven for q

congruent to 2 mod 3, which in this case Λ would be built from linear codes over $\mathbb{F}_{q^2}$.

Corollary 21. *A lattice Λ drawn from an $(n, k, q, \mathbb{Z}[\omega])$ ensemble, where $k < n$ but grows faster than $\log^2 n$ and where k, q satisfy (3.3) and (3.4) is good for quantization, i.e.,*

$$G(\Lambda) \to \frac{1}{2\pi e} \tag{3.53}$$

in probability as $n \to \infty$.

Proof. It was shown in [11] that a lattice ensemble which is good for covering is necessarily good for quantization. Thus from Theorem 19, the result follows. □

3.2.3 Nested $\mathbb{Z}[\omega]$-lattices obtained from Construction A

Nested $\mathbb{Z}[\omega]$-lattices can be obtained from Construction-A very similar to $\mathbb{Z}$-lattices as mentioned in Section 2.2.2. The coarse lattice Λ is obtained through Construction-A as mentioned in Section 3.2.2 with a corresponding generator matrix $\mathbf{B}$. For a given $\mathbf{G} \in \mathbb{F}_q^{n \times k}$, denote Λ' as the corresponding $\mathbb{Z}[\omega]$-lattice obtained through Contruction-A using $\mathbf{G}$ as the generator matrix of the underlying linear code. Generate the $\mathbb{Z}[\omega]$-lattice Λ_f as $\Lambda_f = \mathbf{B}\Lambda'$. It can be observed that $\Lambda \subset \Lambda_f$ with a coding rate of $\frac{k}{2n} \log q$. Given $n,\ k,\ q$ and Λ where Λ is a $\mathbb{Z}[\omega]$-lattice obtained from Construction-A, we define the $(n, k, q, \Lambda, \mathbb{Z}[\omega])$ ensemble as the set of lattices obtained from Λ and Construction-A as previously mentioned where for each of these lattices, the elements of the generator matrix of the underlying linear code $\mathbf{G}_{ij}$ is i.i.d with a uniformly distribution over $\mathbb{F}_q$.

Theorem 22. *There exists of a pair of nested $\mathbb{Z}[\omega]$-lattices where the coarse lattice is good for covering and the fine lattice achieves the Poltyrev limit.*

Proof. For this proof, we build nested $\mathbb{Z}[\omega]$-lattices as mentioned above. Using our result from Theorem 19, we pick a coarse lattice Λ which is good for covering. We then pick Λ_f from the $(n, k, q, \Lambda, \mathbb{Z}[\omega])$ ensemble as described in Section 3.2.3 and show that the Minkowski-Hlawka theorem can be proven for this ensemble [15]. In the detailed proof provided in Appendix A.1, it can be observed that a lattice Λ_f picked from the $(n, k, q, \Lambda, \mathbb{Z}[\omega])$ ensemble achieves the Poltyrev limit as long as the generator matrix $\mathbf{B}$ of Λ is full rank. We would like to note that this result is a more generalized version of what was stated in [15] where $\mathbf{B}$ was assumed to be an identity matrix. One of the consequences of picking an arbitrary full rank matrix $\mathbf{B}$ would be that $\mathcal{V}_\Lambda$ might stretch out in some dimensions while shrinking in others. Nonetheless as long as the growth of q ensures that exactly one element in the kernel of $\tilde{\sigma}$ is contained in the bounded region, the result holds.

□

Now, we are ready to state the main theorem in this chapter.

Theorem 23. *At relay m, given $\underline{h}_m$ and $\underline{a}_m$, a computation rate of*

$$\mathcal{R}(\underline{h}_m, \underline{a}_m) = \log^+ \left(\left(\|\underline{a}_m\|^2 - \frac{P|\underline{h}_m^H \underline{a}_m|^2}{1 + P\|\underline{h}_m\|^2} \right)^{-1} \right), \tag{3.54}$$

where $\underline{a}_{ml} \in \mathbb{Z}[\omega]$, is achievable.

Proof. Using the result from Theorem 22, a fine $\mathbb{Z}[\omega]$-lattice Λ_f and a coarse $\mathbb{Z}[\omega]$-lattice Λ, which is nested in Λ_f with a corresponding coding rate $\frac{R}{2} = \frac{k}{2n} \log q$, is chosen such that Λ_f achieves the Poltyrev limit and Λ is good for covering. Both Λ and Λ_f are scaled such that $\sigma_\Lambda^2 = P$. Following this, the lattice codebook $\Lambda_f \cap \mathcal{V}_\Lambda$ is constructed.

Source node l maps its information vector $\underline{w}_l \in \mathbb{F}_q^k$, where $q = |\varrho|^2$ and ϱ is an

Eisenstein prime, to a lattice codeword $\underline{t}_l \in \Lambda_f \cap \mathcal{V}_\Lambda$, respectively, via a bijective mapping ψ,

$$\underline{t}_l = \psi(\underline{w}) = \left[\mathbf{B}\varrho^{-1}\sigma^{-1}(\mathbf{G}\underline{w})\right], \tag{3.55}$$

where σ was defined in Section 3.2.2. It then constructs a dither vector $\underline{d}_l$, which is uniformly distributed within $\mathcal{V}_\Lambda$ and subtracts this dither vector from the lattice codeword $\underline{t}_l$ and transmits the following:

$$\underline{x}_l = [\underline{t}_l - \underline{d}_l] \mod \Lambda. \tag{3.56}$$

Given a channel coefficient vector $\underline{h}_m \in \mathbb{C}^L$, relay m observes

$$\underline{y}_m = \sum_{l=1}^{L} h_{ml}\underline{x}_l + \underline{z}_m. \tag{3.57}$$

The relay approximates $\underline{h}_m$, in some sense, by an Eisenstein integer vector $\underline{a}_m \in \mathbb{Z}[\omega]^L$ and its goal will be to recover the following:

$$\underline{v}_m = \left[\sum_{l=1}^{L} (a_{ml}\underline{t}_l)\right] \mod \Lambda \tag{3.58}$$

It proceeds by removing the dithers and scaling the observation with α_m, and therefore,

$$\tilde{\underline{y}}_m = \alpha_m \underline{y}_m + \sum_{l=1}^{L} a_{ml}\underline{d}_l \tag{3.59}$$

where α_m is the MMSE coefficient.

Then $\tilde{\underline{y}}_m$ is quantized to the closest lattice point in the fine lattice Λ_f modulo the

coarse lattice Λ and estimates the following:

$$\hat{\underline{v}}_m = \left[Q\left(\tilde{\underline{y}}_m\right)\right] \mod \Lambda \tag{3.60}$$

where Q denotes the quantization with respect to Λ_f.

Note that

$$\left[Q_{\Lambda_f}\left(\tilde{\underline{y}}_m\right)\right] \mod \Lambda = \left[Q_{\Lambda_f}\left(\left[\tilde{\underline{y}}_m \mod \Lambda\right]\right)\right] \mod \Lambda. \tag{3.61}$$

Furthermore,

$$\begin{aligned}
&\left[\tilde{\underline{y}}_m\right] \mod \Lambda \\
&= \left[\sum_{l=1}^{L} \left(\alpha_m h_{ml} \underline{x}_l + a_{ml} \underline{d}_l\right) + \alpha_m \underline{z}_m\right] \mod \Lambda && (3.62) \\
&= \left[\sum_{l=1}^{L} \left(a_{ml} \left[\underline{t}_l - \underline{d}_l\right] \mod \Lambda + \underline{d}_l\right)\right. \\
&\qquad \left. + \sum_{l=1}^{L} \left[\left(\alpha_m h_{ml} - a_{ml}\right) \underline{x}_l + \alpha_m \underline{z}_m\right]\right] \mod \Lambda && (3.63) \\
&= \left[\underline{v}_m + \sum_{l=1}^{L} \left(\alpha_m h_{ml} - a_{ml}\right) \underline{x}_l + \alpha_m \underline{z}_m\right] \mod \Lambda && (3.64) \\
&= \left[\underline{v}_m + \underline{z}_{eq}\right] \mod \Lambda && (3.65)
\end{aligned}$$

As seen in (3.64), self interference occurs as a result of approximating $\underline{h}_m$ by $\underline{a}_m$. Note that due to dithering, $\underline{z}_{eq,m}$ in (3.65) is uncorrelated with the $\underline{x}_l$'s. Furthermore since Λ is good for covering and the dithers are uniformly distributed in $\mathcal{V}_\Lambda$, the probability density function of $\underline{z}_{eq,m}$ is upper-bounded by a zero-mean Gaussian with a variance that approaches $|\alpha_m|^2 + P||\alpha_m \underline{h}_m - \underline{a}_m||^2$ multiplied by a constant as $n \to \infty$ ([6,

Lemma 8]). Finally, the relay maps $\underline{\hat{v}}_m$ to $\underline{\hat{f}}_m$ via ψ^{-1}, where

$$\psi^{-1}\left(\underline{\hat{v}}_m\right) = \underline{\hat{f}}_m = \left(\mathbf{G}^T\mathbf{G}\right)^{-1}\mathbf{G}^T\sigma\left(\varrho\left(\left[\mathbf{B}^{-1}\underline{\hat{v}}_m \mod \Lambda\right]\right)\right) = \bigoplus_{l=1}^{L} b_{ml}\underline{\hat{w}}_l, \tag{3.66}$$

and $b_{ml} = \sigma\left(a_{ml}\right)$. The remaining steps of the proof would then be identical to the steps in the proof of Theorem 5 in [6]. We would like to note that the error probability $\Pr\left(\underline{z}_{eq} \notin \mathcal{V}_{\Lambda_f}\right)$ goes to zero as $n \to \infty$, however this decay is not necessarily exponential in n, since we have only proven the existence of $\mathbb{Z}[\omega]$-lattices which achieve the Poltyrev limit and this result does not provide information about the error exponents of such lattices. Nonetheless, it is sufficient to achieve the computation rate in (3.54). □

3.2.4 Numerical results

In this section, we present some numerical results on the achievable computation rates with $\mathbb{Z}[\omega]$-lattices and compare them to the maximum achievable rates with $\mathbb{Z}$-lattices. We consider the case of $L = 2$ transmitters and there is $M = 1$ relay. For a given channel coefficient vector $\underline{h}$, let $\mathcal{R}_E(\underline{h})$ and $\mathcal{R}_G(\underline{h})$, denote the maximum achievable rate using $\mathbb{Z}[\omega]$-lattices and $\mathbb{Z}$-lattices, respectively, i.e.,

$$\mathcal{R}_E(\underline{h}, P) = \max_{\underline{a}\in\mathbb{Z}[\omega]^2} \log^+\left(\left(\|\underline{a}\|^2 - \frac{P|\underline{h}^H\underline{a}|^2}{1+P\|\underline{h}\|^2}\right)^{-1}\right) \tag{3.67}$$

and

$$\mathcal{R}_G(\underline{h}, P) = \max_{\underline{\tilde{a}}\in\mathbb{Z}[i]^2} \log^+\left(\left(\|\underline{\tilde{a}}\|^2 - \frac{P|\underline{h}^H\underline{\tilde{a}}|^2}{1+P\|\underline{h}\|^2}\right)^{-1}\right). \tag{3.68}$$

In Fig. 3.3, we fix the channel realization to be $\underline{h} = [1.4193 + j0.2916; 0.1978 + j1.5877]$ and compare $\mathcal{R}_E(\underline{h}, P)$, $\mathcal{R}_G(\underline{h}, P)$ for different SNRs. For this particular $\underline{h}$,

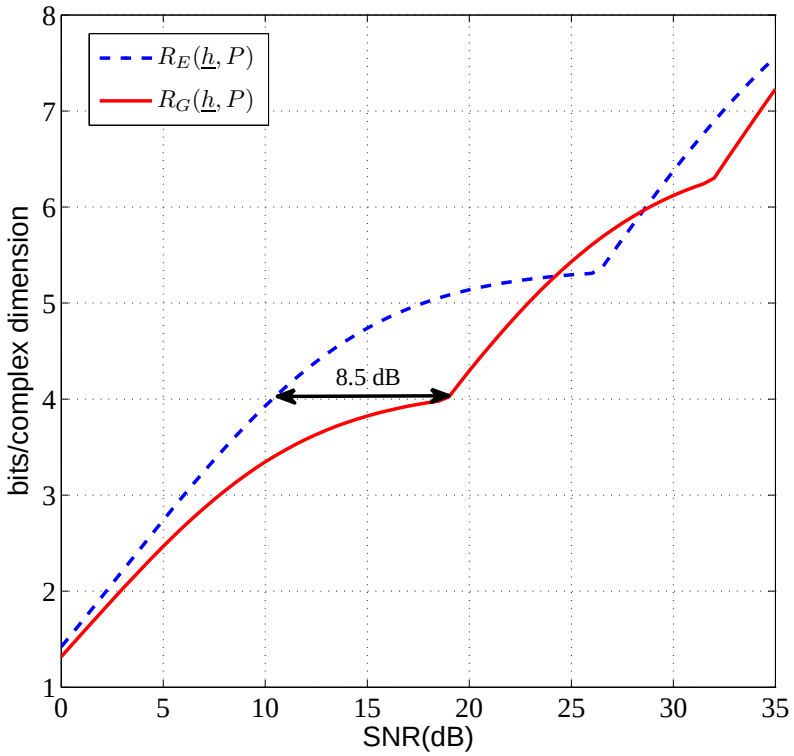

Figure 3.3: $\mathcal{R}_E(h, P)$ vs $\mathcal{R}_G(h, P)$ for a fixed h

it can be observed that $\mathbb{Z}[\omega]$-lattices can achieve substantially higher rates than $\mathbb{Z}$-lattices in the medium SNR regime. We would like to note that this is not necessarily the case for every channel realization, nonetheless it is a perfect example of how channel realizations affect the performance of $\mathbb{Z}[\omega]$-lattices and $\mathbb{Z}$-lattices. Therefore, a larger number of channel realizations should be considered in order to make a fair comparison of their performance in the average sense.

In Fig. 3.4, we fix $h_1 = 1$ and choose h_2 such that $\Re(h_2), \Im(h_2) \in [-4, 4]$ and choose the SNR to be 10 dB. We would also like to note that we do not impose a probability distribution on h_2. For each pair $(h_1 = 1, h_2)$, we plot the region where $\mathcal{R}_G(\underline{h}) > \mathcal{R}_E(\underline{h})$, $\mathcal{R}_G(\underline{h}) < \mathcal{R}_E(\underline{h})$ or $\mathcal{R}_G(\underline{h}) = \mathcal{R}_E(\underline{h})$. For the total number of

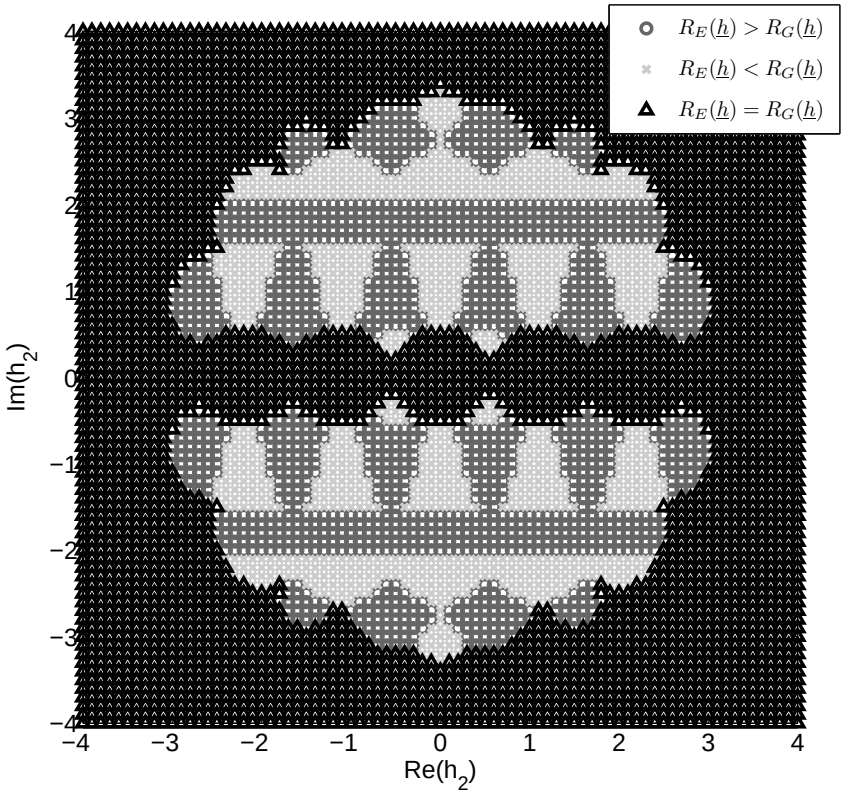

Figure 3.4: $\mathcal{R}_E(h, P)$ vs $\mathcal{R}_G(h, P)$ for a range of h

realizations considered, $\mathcal{R}_E > \mathcal{R}_G$, $\mathcal{R}_E < \mathcal{R}_G$. and $\mathcal{R}_E = \mathcal{R}_G$ for 22.6%, 15.9%, and 61.5% of the realizations, respectively. One might expect that $\mathbb{Z}[\omega]$-lattices would attain a greater maximum achievable rate when h_2 is closer to an Eisenstein integer, $\mathbb{Z}$-lattices would attain a greater maximum achievable rate when h_2 is closer to a Gaussian integer and both lattices would achieve the same maximum achievable rate when h_2 is closer to a natural integer. However as seen from Fig. 3.4, other factors also contribute to the maximum achievable rate. For example when $\|h_2\| \gg \|h_1\|$ or $\|h_2\| \ll \|h_1\|$, the relay chooses $a_1 = 0, \|a_2\| = 1$ or $\|a_1\| = 1, \|a_2\| = 0$, respectively since treating the other transmitted signal as noise (decode-and-forward) results

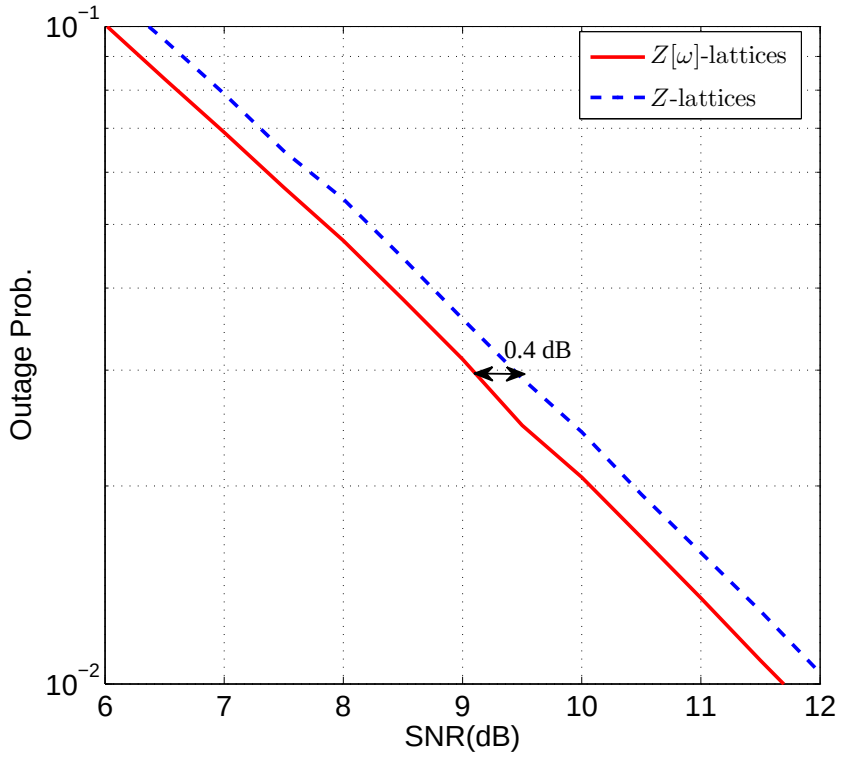

Figure 3.5: Outage probability of $\mathbb{Z}[\omega]$-lattices vs $\mathbb{Z}$-lattices

in maximum achievable rate. Also, the MMSE scaling coefficient α plays a very important role as seen in (2.28), (2.29) and (3.59). Note that (3.67) and (3.68) can be written as

$$\mathcal{R}_E(\underline{h}, P) = \max_{\underline{a} \in \mathbb{Z}[\omega]^2} \log^+ \left(\frac{1 + P\|\underline{h}\|^2}{\|\underline{a}\|^2 + P\left(\|\underline{a}\|^2\|\underline{h}\|^2 - |\underline{h}^H\underline{a}|^2\right)} \right) \tag{3.69}$$

and

$$\mathcal{R}_G(\underline{h}, P) = \max_{\tilde{\underline{a}} \in \mathbb{Z}[\omega]^2} \log^+ \left(\frac{1 + P\|\underline{h}\|^2}{\|\tilde{a}\|^2 + P\left(\|\tilde{\underline{a}}\|^2 |\underline{h}\|^2 - |\underline{h}^H \tilde{\underline{a}}|^2\right)} \right), \tag{3.70}$$

respectively.

As one can see from the denominators in (3.69) and (3.70), it is desirable to align $\underline{a}$ ($\tilde{\underline{a}}$) with $\underline{h}$ as much as possible in order to minimize the second term. However, when $\underline{h} \notin \mathbb{Z}^2$,$\underline{h} \notin \mathbb{Z}[\omega]^2$, or the elements of $\underline{h}$ can not be written as the ratio of Gaussian integers or Eisenstein integers, or $\underline{h}$ is not a rotated version of a Gaussian integer vector or Eisenstein integer vector, $\|\underline{a}\| \to \infty$ ($\|\tilde{\underline{a}}\| \to \infty$) for perfect alignment. Unfortunately, this results in the first term of the denominator to grow and hence there is a tradeoff. Therefore even though h_2 might be closer to an Eisenstein integer (Gaussian integer), i.e. $\underline{h}$ is aligned better with a vector in $\mathbb{Z}[\omega]^2$ ($\mathbb{Z}^2$), the magnitude of this vector might be too large and thus a larger computation rate may be achieved by choosing $\underline{a} \in \mathbb{Z}^2$ ($\tilde{\underline{a}} \in \mathbb{Z}[\omega]^2$)

Given a target rate R_T and a probability distribution $\mathcal{P}$ on $\underline{h}$, i.e. $\underline{h} \sim \mathcal{P}$, we define the outage event of using $\mathbb{Z}$-lattices and $\mathbb{Z}[\omega]$-lattices as $\mathcal{R}_G(\underline{h}) < R_T$ and $\mathcal{R}_E(\underline{h}) < R_T$, respectively. In Fig. 3.5, we plot the outage probability with $\mathbb{Z}[\omega]$-lattices and $\mathbb{Z}$-lattices as a function of SNR (P) where $\Re(h_1), \Im(h_1), \Re(h_2), \Im(h_2) \sim \mathcal{N}(0, 1/2)$. As in Fig. 3.3, $SNR = 10\log_{10}(P)$. We average over 10000 realizations of $\underline{h}$ at each SNR and choose the target rate to be $R_T = 1.4$ bits/symbol/Hz. As seen in Fig. 3.5, there is a 0.4 dB gain from using $\mathbb{Z}[\omega]$-lattices instead of $\mathbb{Z}$-lattices in terms of outage performance. We would like to note that this gain comes with no additional computational complexity.

3.3 Separation-based coding scheme for compute-and-forward

In this section, we propose a separation based compute-and-forward (SBCF) scheme that has an encoding and decoding complexity comparable to widely used error-correcting codes for practical implementations. In the SBCF scheme, we employ lattice codes constructed from linear codes over a prime-sized field $\mathbb{F}_q$ that are mapped to constellations obtained from lattice partitions over $\mathbb{Z}[\omega]$. This mapping is chosen such that a ring homomorphism is satisfied between the lattice partition and $\mathbb{F}_q$. Hence, these lattice codes are essentially finite subsets of lattices built with Construction A. In order to decode a function of transmitted messages at the relay, we perform soft-output demodulation based on the channel itself and the chosen function and then forward the posterior probabilities to a practically implementable decoder. Therefore, the two main differences of the SBCF scheme from the framework in [6] are the absence of additional noise from approximating the channel by an integer vector and the utilization of a decoder much more practical than lattice decoding. A schematic of the proposed encoder and decoder for two transmitters and one relay is shown in Fig. 3.6. For the remainder of this chapter, we shall assume that there are two transmitters and one relay.

3.3.1 An algorithm for constructing and labeling $\mathcal{M}$

For large values of q it is not a trivial task to determine the ring isomorphism σ. Therefore in this section, we provide a simple algorithm to assign elements in $\mathcal{M}$ to elements in $\mathbb{F}_q$.

1. Given a natural prime q congruent to 1 mod 3 and the corresponding Eisenstein prime ϱ, $\mathbb{Z}[\omega]/\varrho\mathbb{Z}[\omega]$

2. Initialize an empty set $\bar{\mathcal{M}}$.

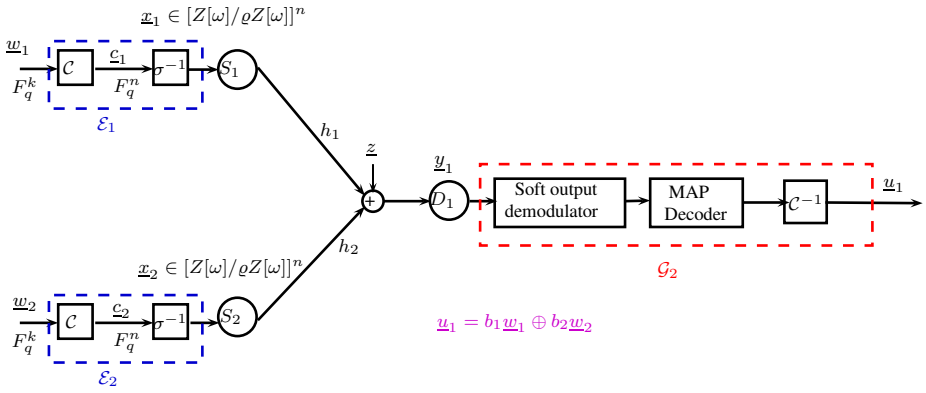

Figure 3.6: Encoder and decoder for proposed scheme

3. Set 0 as the first element in $\bar{\mathcal{M}}$ and label it as $0 \in \mathbb{F}_q$, i.e., $\bar{\mathcal{M}}[1] = 0$ where $\bar{\mathcal{M}}[i]$ denotes the i^{th} element of $\bar{\mathcal{M}}$.

4. Set 1 as the second element in $\bar{\mathcal{M}}$ and label it as $1 \in \mathbb{F}_q$, i.e., $\bar{\mathcal{M}}[2] = 1$.

5. **for** $i = 2 : q - 1$

   $\bar{\mathcal{M}}[i+1] = \bar{\mathcal{M}}[i] + 1 \mod \varrho\mathbb{Z}[\omega]$

   end

Note that at the end of the algorithm, the labeling of each element in $\bar{\mathcal{M}}$ is simply determined by its index. Finally, each element in $\bar{\mathcal{M}}$ is scaled by γ (3.71) in order to satisfy the power constraint.

3.3.2 Encoder for the SBCF scheme

A schematic of the encoder and decoder for the SBCF scheme is shown in Fig. 3.6. Suppose that $\underline{u}_1, \underline{u}_2 \in \mathbb{F}_q^k$ where $q = |\varrho|^2$ is a natural prime congruent to 1 mod 3 and ϱ is an Eisenstein prime. Each source node uses a (n, k) linear code $\mathcal{C}$ over $\mathbb{F}_q$ which encodes $\underline{u}_1, \underline{u}_2$ to $\underline{c}_1, \underline{c}_2$, respectively. We denote $\bar{\mathcal{M}}$ as the coset leaders of

$\mathbb{Z}[\omega]/\varrho\mathbb{Z}[\omega]$ with minimum Euclidean metric and scale it by

$$\gamma = \frac{P}{\mathbb{E}\left(\|x\|^2\right)}, \tag{3.71}$$

which results in $\mathcal{M} = \gamma\bar{\mathcal{M}}$ so that the power constraint is satisfied. Note that $\mathbb{F}_q \cong \mathbb{Z}[\omega]/\varrho\mathbb{Z}[\omega]$ and there is a bijective mapping $\sigma : \bar{\mathcal{M}} \to \mathbb{F}_q$, which is a ring isomorphism. Then, the transmitters map their codeword components $\underline{c}_1^{(i)}, \underline{c}_2^{(i)}$ to the corresponding constellation points $\underline{x}_1^{(i)} = \sigma^{-1}(\underline{c}_1^{(i)}), \underline{x}_2^{(i)} = \sigma^{-1}(\underline{c}_2^{(i)})$, respectively, and transmit $\underline{x}_1, \underline{x}_2 \in \mathbb{C}^n$. We would like to note that $\mathcal{M}$ was constructed based on $\mathbb{Z}[\omega]/\varrho\mathbb{Z}[\omega]$ for better shaping gain.

3.3.3 Decoder for the SBCF scheme

The relay observes

$$\underline{y}_1 = h_1\underline{x}_1 + h_2\underline{x}_2 + \underline{z}. \tag{3.72}$$

Suppose that the relay chooses equation coefficients $b_1, b_2 \in \mathbb{F}_q$ and decodes to the function $f(\underline{u}_1, \underline{u}_2) = b_1\underline{u}_1 \oplus b_2\underline{u}_2$.

Given b_1, b_2 and the variance of $\underline{z}$, namely $\theta^2 = 1$, the relay implements an optimal soft-output demodulator which computes the *a posteriori* probabilities given by

$$p\left(\hat{\underline{c}}^{(i)} = c \middle| \underline{y}_1^{(i)}\right) = \frac{\sum\limits_{(c_1', c_2'):b_1c_1' \oplus b_2c_2' = c} e^{-\left\|h_1\sigma^{-1}(c_1') + h_2\sigma^{-1}(c_2') - \underline{y}_1^{(i)}\right\|^2}}{\sum\limits_{(c_1', c_2') \in \mathbb{F}_q^2} e^{-\left\|h_1\sigma^{-1}(c_1') + h_2\sigma^{-1}(\underline{c}_2') - \underline{y}_1^{(i)}\right\|^2}} \tag{3.73}$$

for all $c \in \mathbb{F}_q$ and for each codeword dimension i. Then, the relay decodes to

$$\arg\max_{\underline{\hat{c}} \in \mathcal{C}} \prod_{i=1}^{n} p\left(\hat{\underline{c}}^{(i)} \middle| \underline{y}_1^{(i)}\right). \tag{3.74}$$

We would like to point out that the relay does not take into account that $\underline{c}_1$ and $\underline{c}_2$ are valid codewords. Instead, it attempts directly to decode to a valid codeword $\underline{\hat{c}}$ which is an estimate of $b_1\underline{c}_1 \oplus b_1\underline{c}_2$.

3.3.4 Achievable computation rate

In this subsection, we will discuss what the achievable information rates are for the SBCF scheme. Given $b_1, b_2 \in \mathbb{F}_q$, the computation rate $I(Y; b_1C_1 \oplus b_2C_2)$ is achievable. Obtaining a closed form solution of this achievable rate is not an easy task since it involves computing the entropy of Gaussian mixtures , nonetheless it can be evaluated quite accurately using Monte-Carlo methods. Finally given P, q and $\underline{h}$, we denote $\mathcal{R}_L(\underline{h}, P, q)$ as

$$\mathcal{R}_L(\underline{h}, P, q) = \max_{b_1, b_2 \in \mathbb{F}_q} I(Y; b_1C_1 \oplus b_2C_2). \tag{3.75}$$

3.3.5 The SBCF scheme with LDPC codes

In order to approach $\mathcal{R}_L(\underline{h}, P)$ arbitrarily closely for a given channel coefficient vector $\underline{h}$ and power constraint P , $\mathcal{C}$ can be chosen as a (n, k) LDPC code over $\mathbb{F}_q$ where $n \to \infty$. A message passing algorithm can be used for decoding as follows. The algorithm is initialized at the variable nodes by computing the q dimensional posterior probability vector $p(\underline{\hat{c}}^{(i)} = c \big| \underline{y}_1^{(i)})$ for all $c \in \mathbb{F}_q$, where $p(\underline{\hat{c}}^{(i)} = c \big| \underline{y}_1^{(i)})$ is the same as (3.73), for each variable node (i) and sent to the check nodes. Once the

initialization is completed, the remaining steps would be identical to the message passing algorithm for decoding any (n, k) non-binary LDPC code over $\mathbb{F}_q$ [35], Ch.7.

The main advantage of using our proposed scheme is that the demodulation and decoding is completely separated. The coding gain is related entirely with the performance of the linear code that we use and the shaping gain is determined by the constellation $\mathcal{M}$ which each codeword component is mapped to. Unlike in (3.64), h_1, h_2 is not approximated by $a_1, a_2 \in \mathbb{Z}[\omega]$. Instead, an optimal soft-output demodulator is used which does not introduce additional self interference. Hence, SBCF has the potential to achieve higher computation rates than Nazer and Gastpar's scheme in [6].

3.4 Simulation results

In this section, we first compute $\mathcal{R}_E(\underline{h}, P)$ and $\mathcal{R}_L(\underline{h}, P, q)$ for $q \in \{7,\ 19,\ 37,\ 241\}$ with $\left\{\varrho \in 2 - j\sqrt{3},\ 4 - j\sqrt{3},\ 5 - j2\sqrt{3},\ 7 - j8\sqrt{3}\right\}$, respectively, as a function of SNR (P) for a given channel realization $\underline{h}$.

As seen in Fig. 3.7 for a given $\underline{h} = [1.4193 + j0.2916; 0.1978 + j1.5877]$ and P, $\mathcal{R}_L(\underline{h}, P, q)$ was able to surpass $\mathcal{R}_E(\underline{h}, P)$ locally in the vicinity of 25 dB as q was increased. Note that $\mathbb{Z}[\omega]$-lattices are employed in order to construct both coding schemes. Unlike the results in Fig. 3.3, the higher achievable rate for the SBCF scheme can not be attributed to $\underline{h}$ being better approximated by an Eisenstein integer vector. Therefore, we believe that higher rates were achievable in the SBCF scheme due to the fact that the decoder implements a soft output demodulator which does not introduce additional noise from approximating the channel by an integer vector.

3.5 Conclusion

In this chapter, we have shown the existence of lattices over Eisenstein integers that are simultaneously good for quantization and are Poltyrev achieving. These

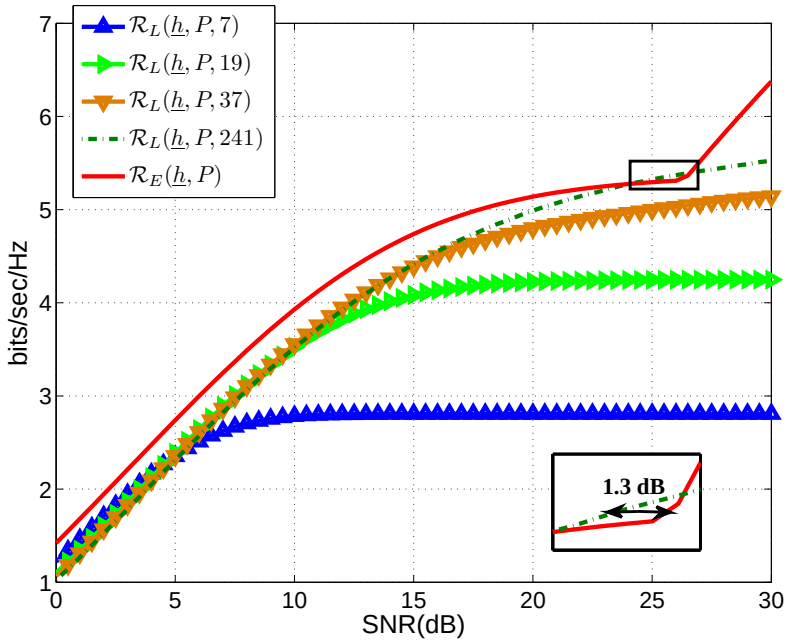

Figure 3.7: Theoretically achievable rates for a given h

lattices were then used to generate lattice codes over Eisenstein integers for compute-and-forward. These lattice codes enable the relays to decode to linear combinations of lattice points with Eisenstein integer coefficients. Numerical results suggest that on average, lattice codes over Eisenstein integers can achieve higher computation rates than lattice codes over integers. We have also proposed practically implementable separation-based coding scheme where a linear code is used for channel coding and a constellation generated from $\mathbb{Z}[\omega]$-lattice partitions (with a small dimension) is adopted for modulation. This separation has allowed us to keep the constellation size small so that optimal demodulation is feasible. Therefore, since the separation-based coding scheme does not introduce additional noise from approximating the channel by an integer vector, we were able to achieve higher computation rates than the framework in [6].

4. SCLDA LATTICE CODES BASED ON CONSTRUCTION A*

In this chapter, motivated by the fact that binary spatially-coupled LDPC codes can achieve capacity under message passing for many channels [23], we construct low-density Construction A (LDA) lattices over integers and Eisenstein integers by choosing the underlying linear code to be a non-binary spatially-coupled LDPC code. We refer to these lattices as spatially-coupled LDA (SCLDA) lattices. We empirically show that the message-passing decoding thresholds for these lattices is close very close to the Polytrev limit. Specifically, Monte Carlo simulations show that spatially-coupled LDA lattices over Eisenstein integers can approach the Poltyrev limit as closely as 0.08 dB ignoring the rate loss due to termination (or 0.19 dB including the rate loss) for a codeword length of 1.29×10^6. Encouraged by these results, we construct spatially-coupled lattice *codes* over Eisenstein integers for the compute-and-forward problem. For a specific channel realization, simulation results show that the message-passing decoding threshold for this code ensemble is within 0.28 dB from the theoretically achievable computation rate and is within 1.06 dB from Nazer and Gastpar's achievable computation rate over Eisenstein integers.

4.1 Related work

Lattice codes have been shown to be optimal for many problems in communications including the point-to-point additive white Gaussian noise (AWGN) channel and coding with side information problems such as the Wyner-Ziv problem or dirty paper coding problem [9], [29]. The construction of optimal lattice codes for these problems often requires a lattice (infinite set of points) that is good for channel

*Reprinted with permission from "Spatially-Coupled Low Density Lattices based on Construction A with Applications to Compute-and-Forward" by N. E. Tunali, K. R. Narayanan, and H. D. Pfister, 2013. Information Theory Workshop, pp. 1-5, copyright [2013] by IEEE.

coding. This is often measured using Poltyrev's idea of the unconstrained AWGN channel. Specifically, the maximum noise variance that a lattice can tolerate while maintaining reliable communication over the point-to-point channel is called the Poltyrev limit [18] and lattices which can achieve the Poltyrev limit are referred to as *Poltyrev good* in the literature. Loeliger showed the existence of lattices that are Poltyrev good by means of Construction A in [15].

Compute-and-forward is a novel relaying paradigm in wireless networks where relays decode functions of signals transmitted from multiple transmissions and forward them to a central destination [24], [6]. Since lattices are closed under integer addition, they are an ideal candidate to build coding schemes to implement a compute-and-forward scheme and the decoding functions can be chosen to be integer combinations. When channel state information is not available at the transmitters, an effective way to implement a compute-and-forward scheme is to allow the relays to adaptively choose the integer coefficients depending on the channel coefficients. Nazer and Gastpar have analyzed such a scheme which uses lattices over integers and derived achievable information rates in [6]. In [7], Feng, Silva and Kschischang have introduced an algebraic framework for designing good lattice codes which allow the recovery of linear combinations of transmitted signals over a finite field. In [28], Nazer and Gastpar's scheme was extended to lattices over Eisenstein integers and in some cases, improved information rates were shown to be achievable.

Poltyrev-good lattices obtained from Construction A play a crucial role in constructing coding schemes that can achieve high computation rates in compute-and-forward. In [26], lattices based on Construction A were built using low density parity check (LDPC) codes and such lattices were referred to as LDA lattices. Pietro *et. al.* proved that LDA lattices can achieve the Poltyrev limit under maximum-likelihood (ML) decoding in [27]. While this result is interesting, the question of whether the

Polytrev limit can be achieved using message passing decoding is still open. Prior simulation results by Pietro *et. al.* in [26] show that a symbol error rate of 10^{-6} can be achieved using LDA lattices in 10000 dimensions with message passing decoding at a gap of 0.7 dB from the Poltyrev limit. In [28], the performance of LDA lattice codes for the compute-and-forward problem was empirically shown to be 0.8 dB away from the corresponding information-theoretic limit. In this chapter, we propose a lattice construction that provides improved performance over the results in [26] and [28].

4.2 Background

4.2.1 Poltyrev limit

Let $\underline{z}$ be an n-dimensional independent and identically distributed (i.i.d) Gaussian vector, $\underline{z} \sim \mathcal{N}\left(\underline{0}, \sigma_{\underline{z}}^2 \mathbf{I}\right)$. Suppose that a lattice point $\underline{\lambda} \in \Lambda$ is transmitted across an AWGN channel and let $\underline{y}$ be the received signal given by:

$$\underline{y} = \underline{\lambda} + \underline{z}. \tag{4.1}$$

The ML decoder decodes to the lattice point nearest in Euclidean distance to $\underline{y}$, which results in the following probability of decoding error:

$$P_e\left(\Lambda, \underline{z}\right) = \Pr\left\{\underline{z} \notin \mathcal{V}_\Lambda\right\}. \tag{4.2}$$

Definition 24 (Poltyrev limit [18])**.** *It was shown in [18] that there exists a Λ in a sufficiently large dimension n such that λ can be decoded with arbitrarily small decoding error $P_e\left(\Lambda, \underline{z}\right)$ if and only if the noise variance σ^2 satisfies $\sigma^2 < \sigma_{max}^2$. The*

maximum noise variance, σ^2_{max} is called the Poltyrev limit and is given by

$$\sigma^2_{max} \triangleq \frac{Vol(\mathcal{V}_\Lambda)^{\frac{2}{n}}}{2\pi e} \tag{4.3}$$

4.2.2 Poltyrev limit of Construction A lattices

We define the $(n, k, q, \mathbb{Z})$ $((n, k, q, \mathbb{Z}[\omega]))$ ensemble as the set of $\mathbb{Z}$ $(\mathbb{Z}[\omega])$-lattices obtained through Construction A where for each of these lattices, $\mathbf{G}_{ij}$ are i.i.d with a uniform distribution over $\mathbb{F}_q$. The Poltyrev limit of a lattice chosen from the $(n, k, q, \mathbb{Z})$ ensemble is given by $\sigma^2_{\max} = \frac{1}{2\pi e} q^{2(1-R)}$ and the corresponding limit for the $(n, k, q, \mathbb{Z}[\omega])$ ensemble is $\sigma^2_{\max} = \frac{\sqrt{3}}{4\pi e} q^{(1-R)}$, where $R = \frac{k}{n}$.

4.2.3 LDA lattices

Definition 25 (LDA lattice [26])**.** *A $\mathbb{Z}$ $(\mathbb{Z}[\omega])$-lattice Λ belongs to the family of LDA lattices over integers (Eisenstein integers), which we refer as LDA $\mathbb{Z}$ $(\mathbb{Z}[\omega])$-lattices, if Λ is chosen from the $(n, k, q, \mathbb{Z})$ $((n, k, q, \mathbb{Z}[\omega]))$ and the underlying discrete codebook $\mathcal{C}$ has an $(n-k) \times n$ sparse parity-check matrix $\mathbf{H}$, in other words $\mathcal{C}$ is an LDPC code. We shall denote the ensemble of such lattices as the* $(n, k, q, \mathbb{Z})$ LDA ensemble or the $(n, k, q, \mathbb{Z}[\omega])$ LDA ensemble*.*

4.3 Spatially-coupled LDA lattices

Motivated by the fact that spatially coupled LDPC codes have been shown to achieve capacity universally under message passing with the assumption that the receiver knows the underlying channel [23], we propose to use spatially-coupled non-binary LDPC codes to build LDA lattices, which we refer to as *spatially-coupled LDA (SCLDA) lattices.*

4.3.1 Construction of spatially-coupled LDA lattices

For constructing spatially-coupled LDA lattices, we choose the underlying LDPC codes over some $\mathbb{F}_q$ from the (d_l, d_r, L) ensemble introduced in [22] Section II-A. This results in a code rate of

$$R = \frac{k-1}{k} - \frac{d_l - 1}{k(2L+1)}. \tag{4.4}$$

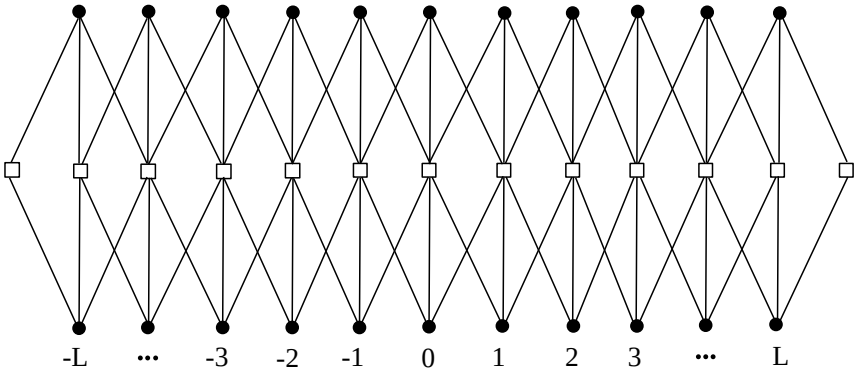

Figure 4.1: Coupled chain of (3,6) protographs

Fig. 4.1 represents a protograph which consists of a coupled chain of $(d_l = 3, d_r = 6)$ protographs. The circles represent the variable nodes and the squares represent the check nodes. In order to build $\mathbf{H}$, M copies are made of this protograph and the edges in Fig. 4.1 impose the connectivity constraint for interconnecting the M copies.

The weights of the edges, are chosen as in [26]. Suppose that row i of $\mathbf{H}$ has a degree of d_i. Denote the vector of non-zero coefficients in this row as $\underline{a}_i$ and denote

each element of $\underline{a}_i$ as $\underline{a}_{ij}$. The condition

$$\underline{a}_{ij} \neq \pm \underline{a}_{ij'}, \quad \forall j, j' \in \{1, \cdots, d_i\}, \quad j \neq j' \tag{4.5}$$

guarantees that the minimum Euclidean distance between any two lattice points λ_1, λ_2 such that $\sigma(\lambda_1)$ and $\sigma(\lambda_2)$ satisfy the ith parity check, exceeds $\sqrt{2}$ [26].

Following the construction of $\mathbf{H}$, the spatially-coupled LDPC code $\mathcal{C}$ is formed and each codeword component is mapped to elements in the quotient ring $\mathbb{Z}/q\mathbb{Z}$ ($\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$) via the ring homomorphism ϕ and tesselated over $q\mathbb{Z}$ ($\pi\mathbb{Z}[\omega]$). The overall construction is summarized in Fig. 4.2.

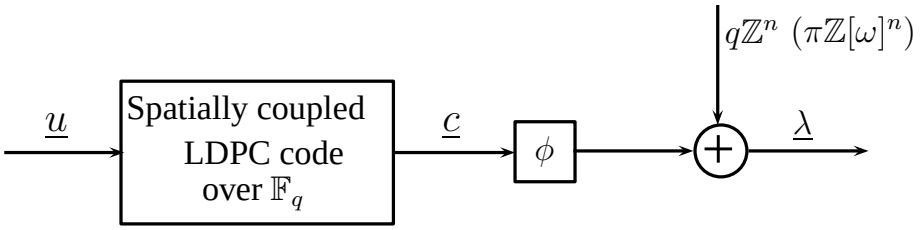

Figure 4.2: Construction of spatially-coupled LDA lattices

4.3.2 Efficient decoding of spatially-coupled LDA lattices

Suppose Λ is chosen from the $(n, k, q, \mathbb{Z})$ LDA ensemble and $\underline{\lambda} \in \Lambda$ is transmitted across an AWGN channel. Let $\underline{y}$ denote the received vector given by

$$\underline{y} = \underline{\lambda} + \underline{z} \tag{4.6}$$

where $\underline{z} \sim \mathcal{N}(\underline{0}, \sigma^2 \mathbf{I})$. The decoding algorithm is a simple extension of the message passing algorithm for decoding non-binary LDPC codes and is nearly identical to the

one in [26]. It consists of the following steps

4.3.2.1 Initialization

For each $\hat{\underline{c}}$, we compute the q-ary probability vector

$$P\left(\hat{\underline{c}}^{(i)}|\underline{y}^{(i)}\right) = \sum_{\hat{\underline{\lambda}}^{(i)} \in \mathbb{Z} | \hat{\underline{\lambda}}^{(i)} \bmod \ q = \hat{\underline{c}}^{(i)}} P\left(\hat{\underline{\lambda}}^{(i)}|\underline{y}^{(i)}\right) \tag{4.7}$$

where

$$P\left(\hat{\underline{\lambda}}^{(i)}|\underline{y}^{(i)}\right) \propto \exp\left(-\frac{\left(\underline{y}^{(i)} - \underline{\lambda}^{(i)}\right)^2}{2\sigma^2}\right). \tag{4.8}$$

Note that there are an infinitely many summands in (4.7) which makes it impossible to compute the exact value.

We approximate the above summation by choosing only one representative from every coset $\mathbb{Z}/q\mathbb{Z}$ that lies closes to $\underline{y}$. Define $\tilde{\underline{\lambda}}^{(i)}$ as:

$$\tilde{\underline{\lambda}}^{(i)} : \underset{\hat{\underline{\lambda}}^{(i)} \in \mathbb{Z} | \hat{\underline{\lambda}}^{(i)} \bmod \ q = \hat{\underline{c}}^{(i)}}{\arg\min} \left|\hat{\underline{\lambda}}^{(i)} - \underline{y}^{(i)}\right| \tag{4.9}$$

Then, (4.7) can be approximated as $P\left(\hat{\underline{c}}^{(i)}|\underline{y}^{(i)}\right) \approx P\left(\tilde{\underline{\lambda}}^{(i)}|\underline{y}^{(i)}\right)$. We would like to note that for large q, this approximation becomes very good.

4.3.2.2 Iterations

Once the initialization process is completed, variable-to-check node messages and check-to-variable node messages can be updates identical to the traditional message passing algorithm over $\mathbb{F}_q$ where q is prime.

4.3.2.3 Decisions at each iteration

Denote the normalized product of all messages that variable node i receive from the check nodes it is connected to at the j^{th} iteration as

$$P^{(j)}\left(\underline{\hat{c}}^{(i)}|\mathcal{C}, \underline{y}\backslash\underline{y}^{(i)}\right). \tag{4.10}$$

The decision for the i^{th} component of $\underline{\lambda}$ at the j^{th} iteration can be written as:

$$\underset{\tilde{\underline{\lambda}}^{(i)}|\tilde{\underline{\lambda}}^{(i)} \bmod q=\hat{\underline{c}}^{(i)}}{\arg\max} P^{(j)}\left(\underline{\hat{c}}^{(i)}|\mathcal{C}, \underline{y}\backslash\underline{y}^{(i)}\right) \cdot P\left(\tilde{\underline{\lambda}}^{(i)}|\underline{y}^{(i)}\right) \tag{4.11}$$

For decoding LDA $\mathbb{Z}[\omega]$-lattices, (4.7), (4.8), and (4.9) should be changed such that $\underline{\lambda}, \underline{z} \in \mathbb{C}^n$. Also, the mod q operation in (4.7), (4.9), and (4.11) should be replaced with the ring homomorphism $\phi(\hat{\underline{\lambda}}^{(i)})$ mentioned in section 4.2.2.

4.3.3 Simulation results of spatially-coupled LDA lattices

In this section, we present simulation results in which we empirically study the thresholds of a spatially-coupled LDA $\mathbb{Z}$-lattice and a spatially-coupled LDA $\mathbb{Z}[\omega]$-lattice with the same underlying $\mathbf{H}$. $\mathbf{H}$ was chosen from the $(d_l = 3, d_r = 6, L = 64)$ ensemble over $\mathbb{F}_{31}$ with a protograph lifting factor of $M = 10000$ and each non-zero element of $\mathbf{H}$ is chosen as mentioned in Section 4.3.1. For the spatially-coupled LDA $\mathbb{Z}[\omega]$-lattice, the Eisenstein prime $\pi = 2 - 3\sqrt{3}j$ is used for generating the ring homomorphism that maps $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ to $\mathbb{F}_{31}$. This choice of parameters result in a code with codeword length 1.29×10^6 and code rate of 0.4922 including the rate loss from the termination. Due to the symmetry in the lattice, the all-zero lattice point is assumed to be transmitted. Instead of plotting the symbol error rate curve, we focus on determining the threshold of the resulting lattice under message passing.

We estimate the threshold by determining the maximum noise variance for which no codeword errors ($\hat{\underline{c}} \neq \underline{0}$) were observed in the simulation of 10 codewords each of length 1.29×10^6 symbols. There is a small difference between the codeword error rate and the probability of decoding to a wrong lattice point for finite q.

Notice that the minimum squared Euclidean distance between any two lattice points in any lattice constructed using Construction A over integers is at most q^2 and that over Eisenstein integers is q. These correspond to the minimum Euclidean distance between any two points in the coset $q\mathbb{Z}$ and $\pi\mathbb{Z}[\omega]$, respectively. When the decoder chooses a wrong lattice point from the same coset, the codeword over the finite field will still be correctly decoded. These events are not counted as errors in our simulations. As q increases, the probability of these events decreases and, hence, does not become a significant issue. For any fixed q, the symbol error rate is lower bounded by $Q\left(\sqrt{\frac{q^2}{4\sigma^2}}\right)$ for $\mathbb{Z}$-lattices and is lower bounded by $Q\left(\sqrt{\frac{q}{4\sigma^2}}\right)$ for $\mathbb{Z}[\omega]$-lattices. For $q = 31$, these are 2.02×10^{-29} for $\mathbb{Z}$-lattices and 1.17×10^{-7} for $\mathbb{Z}[\omega]$-lattices. Thus, there will be an error floor which is not shown in the threshold calculations.

In Table 4.1, thresholds are stated with and without considering the rate loss from the termination. For the results in this table, $q = 31$ and $R = 0.4922$. ${\sigma^2_{\max}}^*$ and Gap* correspond to the Polytrev limit and gap from the Polytrev limit without the rate loss from termination, i.e. $R = 0.5$. If the rate loss from the termination is ignored, the threshold of the spatially-coupled LDA $\mathbb{Z}$-lattice and $\mathbb{Z}[\omega]$-lattice with the specified parameters are 0.11 dB and 0.08 dB from the Poltyrev limit, respectively. This gap increases to 0.34 dB and 0.19 dB away from the Poltyrev limit, respectively if the rate loss from termination is included.

Table 4.1: Thresholds for SCLDA $\mathbb{Z}$ and $\mathbb{Z}[\omega]$-lattices .

Lattice	Threshold	$\sigma^2_{\max}$	Gap	$\sigma^2_{\max}{}^*$	Gap*
$\mathbb{Z}$-lattice	1.7707	1.9149	0.34 dB	1.815	0.11 dB
$\mathbb{Z}[\omega]$-lattice	0.2776	0.2900	0.19 dB	0.2823	0.08 dB

4.4 Spatially-coupled LDA $\mathbb{Z}[\omega]$-lattice codes for CF

Encouraged by the near-Poltyrev-limit performance of spatially-coupled LDA $\mathbb{Z}[\omega]$-lattices, we use them to build lattice codes in order to implement the separation-based framework for compute-and-forward proposed in Chapter 3. 3.3. For the sake of simplicity, we will assume two transmitter 1 relay node model in Fig. 3.6.

4.4.1 Simulation results

In this section, we present the simulation results for the separation-based compute-and-forward scheme that employs a spatially-coupled LDPC code, i.e. the resulting code is a spatially-coupled LDA $\mathbb{Z}[\omega]$-lattice code. We build the underlying LDPC over $\mathbb{F}_7$, corresponding to an Eisenstein prime of $\pi = 2-\sqrt{3}j$, and choose it from the $(d_l = 3,\ d_r = 6,\ L = 64)$ ensemble with a protograph lifting factor of $M = 10000$. This choice of parameters result in a code with codeword length 1.29×10^6 and code rate of 0.4922. Due to the fact that the infinite lattice is not considered in this case, the minimum Euclidean distance of the single parity check code loses its significance. Hence, each non-zero element in the parity check matrix chosen according to a uniform distribution over the set $\{1, 2, 3, 4, 5, 6\}$.

For channel realizations $\underline{h} = [1.4193+0.2916j; 0.1978+1.5877j]$, the computation rate of the proposed scheme is maximized for $b_1 = 1,\ b_2 = 5$ for all SNRs considered. Using the same approach in Section 4.3.3 for estimating thresholds, we have observed the threshold of the spatially-coupled LDA lattice code to be within 0.28 dB from

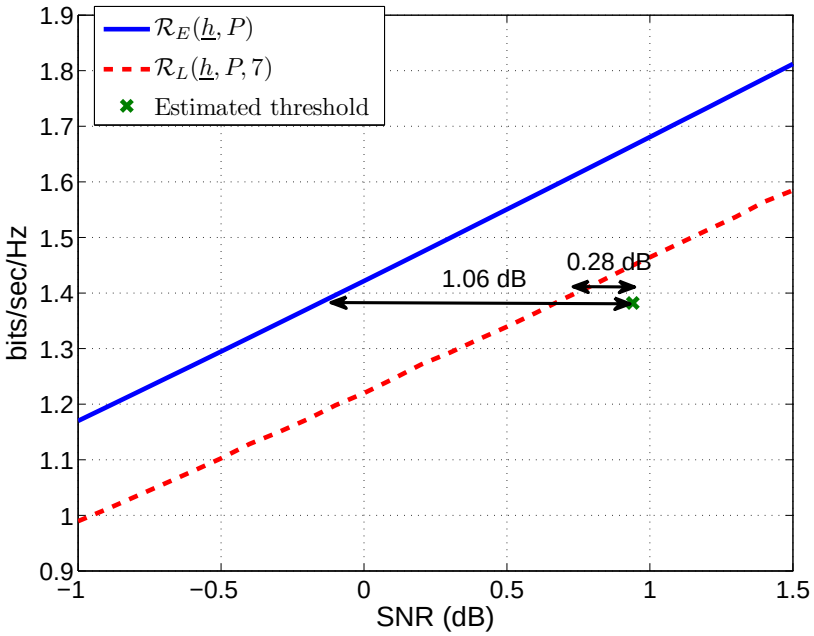

Figure 4.3: Estimated threshold for the spatially-coupled LDA $\mathbb{Z}[\omega]$-lattice code

$\mathcal{R}_L(\underline{h}, P, q)$ and 1.06 dB from $\mathcal{R}_E(\underline{h}, P)$ as seen in Fig. 4.3. We would like to note that if the rate loss from the termination of the code is ignored, the gaps reduce to 0.18 dB and 0.96 dB, respectively. The remaining gap is mainly due to the shaping loss.

5. CONCATENATED SIGNAL CODES FOR COMPUTE-AND-FORWARD*

In this chapter, we present a new coding scheme based on concatenating convolutional lattice codes, also referred to as signal codes, with interleaved low density parity check (LDPC) codes. We derive two decoding algorithms for these codes. In the first one, hard decisions are forwarded from a stack decoder which reaches a certain depth whereas in the second one, soft outputs from a Trellis-based decoder are forwarded. For the point-to-point case, simulation results show that our proposed scheme based on forwarding hard decisions approaches capacity to within 1 dB, whereas forwarding soft decisions approaches capacity to within 0.1 dB. Since these codes belong to the family of lattice codes, this facilitates their use as a coding scheme for the compute-and-forward paradigm. Simulation results show that our proposed coding scheme can approach the theoretically achievable exchange rates for compute-and-forward over the bidirectional relay network using nested lattice codes, which is $\log(1/2 + SNR)$ [24], as close as 0.5 dB in the medium SNR regime.

5.1 Introduction

Compute-and-forward is an information forwarding paradigm in wireless relay networks in which relays directly decode to functions of signals transmitted from multiple transmitters, i.e. integer linear combinations, and forward them to a central destination such that the central destination can recover each individual signal from the transmitters. Due to the fact that lattices are closed under integer addition, lattice codes are naturally suited to decoding integer linear combinations of transmitted signals.

*Reprinted with permission from "Concatenated Signal Codes with Applications to Compute and Forward" by N. E. Tunali and K. R. Narayanan, 2011. Information Theory Workshop, pp. 1-5, copyright [2011] by IEEE.

In [12], Low-Density Lattice Codes (LDLC), which are lattices with sparse parity check matrices, have been introduced and were shown to have near Poltyrev-limit asymptotic symbol error rate (SER)performance in the asymptotic block length. For decoding LDLC, a message passing decoder which passes quantized probability density functions is used. One of the drawbacks of LDLC is its high-complexity decoding algorithm. In order to overcome this disadvantage, a reduced complexity message passing algorithm based on passing Gaussian mixture parameters was introduced in [30]. In order to further enhance the SER performance of LDLC, spatially-coupled LDLC have been introduced by Uchikawa *et. al.* in [38]. Low-density Construction A (LDA) lattices, which are lattices built from LDPC codes through Construction A and also belong to the class of low-density lattices, were introduced by Pietro *et. al.* in [26] and were shown to achieve the Poltyrev limit under ML decoding in [27]. The performance of spatially-coupled LDA lattices and their application to compute-and-forward were studied in [39]. Polar lattices, which are lattices constructed from Polar codes through Construction D, were introduced by Yan *et. al.* in [31] and were shown to achieve the Poltyrev limit under multi-stage decoding. In [13] and [21], convolutional lattice codes, also known as signal codes, which can be thought of as the lattice counterpart of convolutional codes, were introduced by Shalvi *et. al.*. One of the disadvantages of convolutional lattice codes is the lack of good asymptotic SER performance in block length and the utilization of a high complexity sequential decoder in order to approach capacity.

In this chapter, we propose a lattice-based coding scheme, which we refer to as concatenated convolutional lattice codes (CCLC), that is based on concatenating convolutional lattice codes with interleaved LDPC codes in order to achieve good asymptotic SER performance in blocklength and approach capacity without the burden of a high-complexity sequential decoder. The outline of the chapter is

as follows. We first give some background on convolutional lattice codes. We then introduce CCLC, and two different decoding algorithms which are based on forwarding hard decisions and soft outputs to the interleaved LDPC code, respectively. We then employ CCLC for the compute-and-forward paradigm in a bidirectional relay channel.

5.2 Background on convolutional lattice codes

5.2.1 Convolutional lattice codes

Definition 26 (Convolutional Lattice)**.** *Let $\underline{f}$ denote a monic causal filter with transfer function $F(z) = 1 + \sum_{l=1}^{L} f_l z^{-l}$. A convolutional lattice, Λ is defined as $\Lambda = \{\underline{x} = \underline{f} \star \underline{a} : \underline{a} \in \mathbb{Z}[i]^n\}$. The generator matrix of Λ, which we denote as $\mathbf{G} \in \mathbb{C}^{(N+L)\times N}$, can be written as*

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ f_1 & 1 & 0 & \cdots & 0 & 0 & 0 \\ f_2 & f_1 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ f_L & f_{L-1} & f_{L-2} & \cdots & 0 & 0 & 0 \\ 0 & f_L & f_{L-1} & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & f_2 & f_1 & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & f_L & f_{L-1} & f_{L-2} \\ 0 & 0 & 0 & \cdots & 0 & f_L & f_{L-1} \\ 0 & 0 & 0 & \cdots & 0 & 0 & f_L \end{pmatrix}$$

Therefore Λ can also be defined as $\Lambda = \{\underline{x} = \mathbf{G}\underline{a} : \underline{a} \in \mathbb{Z}[i]^n\}$

Definition 27 (Unshaped Convolutional Lattice Code)**.** *Let $\mathcal{M}$ denote an M^2-QAM constellation, where $\Re(\mathcal{M}) = \Im(\mathcal{M}) = \{0, 1, \dots M-1\}$ and let $\underline{a} \in \mathcal{M}^N$. An unshaped convolutional lattice code, which we denote as Λ_C is defined as $\Lambda_C = \{\underline{x} = \underline{f} \star \underline{a} : \underline{a} \in \mathcal{M}^n\}$, or $\Lambda_C = \{\underline{x} = \mathbf{G}\underline{a} : \underline{a} \in \mathcal{M}^n\}$. Hence, $\underline{x}$ can be written as:*

$$x_n = a_n + \sum_{l=1}^{L} f_l a_{n-l} \tag{5.1}$$

for $n = 1, \cdots, N+L-1$ and a_n is assumed to be zero outside the range $n = 1, \cdots, N$.

In [13], the filter coefficients are carefully chosen such that the minimum distance between any two codewords in Λ_C is substantially higher than that of uncoded M^2-QAM. However, this comes at the cost of a higher average energy for Λ_C. In order to reduce the average transmit power and maintain the increased minimum distance, hypercube shaping based on Tomlinson-Harashima precoding can be implemented as follows [20].

Definition 28. *(*Convolutional Lattice Codes with hypercube shaping*):*

Recall that a_n belongs to an M^2-QAM constellation. The shaping operation maps each a_n to b_n via

$$b_n = a_n - Mk_n \tag{5.2}$$

where k_n is a complex integer and is computed as

$$k_n = \left\lfloor \frac{1}{M}\left(a_n + \sum_{l=1}^{L} f_l b_{n-l}\right)\right\rceil \tag{5.3}$$

and $\lfloor x \rceil$ denotes the complex integer closest to x. After k_n and b_n have been computed,

x_n can be computed as

$$x_n = b_n + \sum_{l=1}^{L} f_l b_{n-l} \tag{5.4}$$

which is the equivalent of $\underline{x} = \mathbf{G}\underline{b}$. This shaping method ensures that for every x_n, $\Re(x_n) \in [-\frac{M}{2}, \frac{M}{2})$ and $\Im(x_n) \in [-\frac{M}{2}, \frac{M}{2})$. As $n \to \infty$, it can be shown that $\Re(x_n)$ and $\Im(x_n)$ is uniformly distributed within $[-\frac{M}{2}, \frac{M}{2})$, which results in an average power of $\frac{1}{6}M^2$. Notice that a_n can be determined uniquely from b_n by a modulo M operation. The encoding of Convolutional Lattice Codes is summarized in Fig. 5.1.

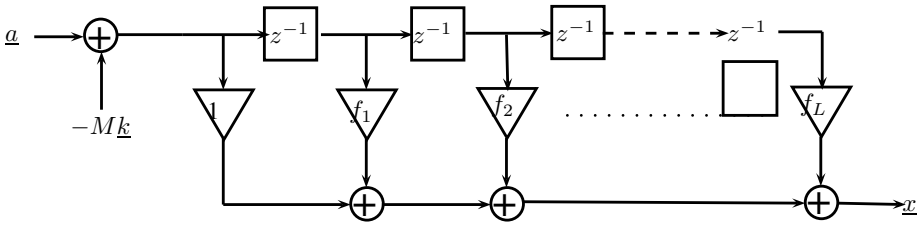

Figure 5.1: Encoding of convolutional lattice codes

5.2.2 Decoding convolutional lattice codes

Assume that each x_n is transmitted over an AWGN channel such that $y_n = x_n + z_n$ where z_n are zero mean, independent and identically distributed (i.i.d) Gaussian random variables. In order to decode to the corresponding $\underline{a}$, the maximum likelihood decoder should maximize

$$L(\underline{y}|\underline{a}) = -\sum_{n} \left| y_n - \sum_{l=0}^{L} f_l b_{n-l}^{a} \right|^2 \tag{5.5}$$

where b_n^a's correspond to hypercube shaped a_n's. In the decoding algorithm proposed in [13], the b_ns are treated as free variables and the decoder attempts to maximize

$$L(\underline{y}|\underline{b}) = -\sum_n \left| y_n - \sum_{l=0}^{L} f_l b_{n-l} \right|^2 \tag{5.6}$$

This decoder is the equivalent of decoding to the nearest lattice point without taking the shaping region into consideration. It can be shown that for lattice codes of large dimensions, disregarding the shaping algorithm does not affect the performance of the decoder.

It can be observed that convolutional codes (or inter-symbol interference channels), and convolutional lattice codes share similar structural properties. Just as convolutional codes, the sequence-wise optimal maximum likelihood decoder of convolutional lattice codes would be the Viterbi Algorithm with at least M^L many Trellis branches. However, hypercube shaping increases the cardinality of b_n to a much larger value than M. Hence, implementing a straightforward Viterbi algorithm is computationally infeasible.

Therefore, suboptimal decoders for convolutional lattice codes were proposed in [13] . One of these suboptimal decoders is the stack decoder which stores the candidate b_n's in a stack and updates the stack after each step by sorting the metrics of the candidates and only allowing S_L of them to remain in the stack where S_L is the maximal stack length [1]. The Fano metric to be used in the stack decoder with Tomlinson-Harashima shaping has been derived in [13] and is given by

$$L(\underline{y}|\underline{b}) = -\sum_n \left[\left| y_n - \sum_{l=0}^{L} f_l b_{n-l} \right|^2 - B \right] \tag{5.7}$$

and

$$B \approx \sigma^2 \cdot \log \frac{4}{\sigma^2} \tag{5.8}$$

where B is the bias term [13].

It can be inferred that convolutional lattice codes do not have good asymptotic SER performance in blocklength, which is undesirable for certain applications. In order to overcome this disadvantage, convolutional lattice codes can be concatenated with LDPC codes. However, a straightforward concatenation would not result in a good coding scheme due to the fact that the failure of the stack decoder results in bursty errors and thus cripples the error correcting capability of the LDPC code. This has motivated us to develop a more sophisticated concatenation scheme and an appropriate decoding scheme which is discussed in the following section.

5.3 Concatenated convolutional lattice codes

5.3.1 Motivation

As we have mentioned before, there is a great similarity between convolutional lattice codes and inter-symbol interference (ISI) channels. In fact, convolutional lattice codes can equivalently be thought of as transmitting QAM symbols through an ISI channel with carefully selected channel coefficients combined with Tomlinson-Harashima precoding. Therefore in order to approach capacity with convolutional lattice codes, we were motivated by various works that focused on designing coding schemes that achieve capacity over ISI channels [2], [3], [4] [5].

In [5], Pfister *et. al.* derive the achievable rates for ISI channels by introducing a coding scheme which uses interleaved multiplexed codes with different rates chosen in a specific manner for the channel and a multi-stage decoder which involves multiple

passes of a BCJR decoder. The structure of this coding scheme can effectively be thought of as interleaved codes with known symbols added between them and hence results in the equivalent channels to become memoryless. In [3], a similar approach is undertaken by using a single interleaved code with the first L columns perfectly known along with a BCJR decoder that passes optimal soft outputs. Once a column is decoded, it is assumed to be perfectly known and the BCJR decoder computes the soft outputs of the next column and forwards them to the interleaved code with the assumption that the previous columns are perfectly known. Hence, the equivalent channels for each column become identical and memoryless. This approach is referred to as BCJR decision feedback equalization (BCJR-DFE) and has been shown to achieve capacity as blocklength tends to infinity under the assumption that the interleaved code is a capacity achieving code. Motivated by this result, we adapt a similar concatenation scheme for convolutional lattice codes.

5.3.2 Encoding concatenated convolutional lattice codes

For encoding concatenated Convolutional Lattice codes, we insert our information letters into a $K \times N_2$ matrix, which we denote as $\mathbf{U}$, and $u_{i,j} \in \mathbb{F}_{M^2}$. Then an LDPC code, which we denote as $\mathcal{C}$, over $\mathbb{F}_{M^2}$ with rate $R = K/N_1$ is used in order to encode each column $\mathbf{U}_i \in \mathbb{F}_{M^2}^K$ to an LDPC codeword $\mathbf{C}_i \in \mathbb{F}_{M^2}^{N_1}$. We denote the matrix of cascaded $\mathbf{C}_i$'s as $\mathbf{C}$. The encoding operation that has been described so far can be expressed as

$$\mathbf{C} = \mathbf{G}_{LC} \cdot \mathbf{U}, \tag{5.9}$$

where $\mathbf{G}_LC$ denotes the $N_1 \times K$ generator matrix of $\mathcal{C}$.

We proceed the encoding process by mapping each element of $\mathbf{C}$ to an M^2-QAM symbol with a bijective mapping $f : \mathbb{F}_{M^2} \to \mathcal{M}$ and denote this matrix as $\mathbf{A}$. We then

encode each row $\mathbf{A}^j \in \mathcal{M}^{N_2}$ to a hypercube shaped convolutional lattice codeword $\mathbf{X}^j \in \mathbb{C}^{N_2+L}$. We denote the matrix of cascaded $\mathbf{X}^j$'s as $\mathbf{X}$. These operations can be expressed as

$$\mathbf{X} = (\mathbf{A} - M\mathbf{K})\,{\mathbf{G}_{CL}}^T, \tag{5.10}$$

where $\mathbf{G}_{CL}$ denotes the generator matrix of a Convolutional Lattice Code and $\mathbf{K}$ denotes the subtracted integer vector as a result of hypercube shaping. The overall encoding operation is thus

$$\mathbf{X} = (f\,(\mathbf{G}_{LC} \cdot \mathbf{U}) - M\mathbf{K})\,{\mathbf{G}_{CL}}^T. \tag{5.11}$$

In order to ensure that the energy of the convolution tail is controlled in the last L columns of $\mathbf{X}$ these elements can be chosen from an uncoded larger QAM constellation as mentioned in [13]. Since we will be analyzing CCLC for asymptotic blocklength in this chapter, we will not take the last L columns of $\mathbf{X}$ into consideration in our analysis.

5.3.3 Decoding concatenated convolutional lattice codes

Suppose a CCLC is transmitted over an AWGN channel such that at the receiver $\mathbf{Y} = \mathbf{X} + \mathbf{Z}$ is observed where $z_{i,j} \sim \mathbb{C}\mathcal{N}(0, \sigma^2)$. With the absence of hypercube shaping, this coding scheme could equivalently be thought of as transmitting interleaved LDPC codes over an ISI channel. As we mentioned in Sec. 5.3.1, the BCJR-DFE equalizer combined with a capacity achieving interleaved code achieves capacity as $N_1 \to \infty$ and $N_2 \to \infty$. However for concatenated convolutional lattice codes, obtaining optimal soft outputs for each column is computationally infeasible since hypercube shaping results in the cardinality of state space to increase sub-

stantially. In order to approach capacity with Concatenated Convolutional Lattice Codes, we propose two suboptimal decoders which we refer to as the hard decision based decoder and soft output based decoder.

5.3.3.1 Hard decision based decoding of CCLC

Once $\mathbf{Y}$ is received, N_1 stack decoders are run in parallel for each row $\underline{y}^i$. Once each stack decoder reaches a depth of τ a hard decision is made on the first symbol for each $\underline{c}^i$, thus making a hard decision on the first column $\underline{c}_1$. Then, the hard decisions for the first column forwarded to a message passing decoder and $\underline{c}_1$ is decoded. If the SNR is higher than the BP threshold of the LDPC code, $\underline{c}_1$ can decoded with very high probability and it can be assumed that it is perfectly known. We then repeat this procedure for the second column $\underline{c}_2$, under the assumption that the the first column is known. Note that the equivalent channel for each element in $\underline{c}_2$ would be identical to the equivalent channel for each symbol of $\underline{c}_1$ and these channels would be memoryless. We continue repeating this procedure for each $\underline{c}_j$ until all $N_2 + L$ columns are decoded.

5.3.3.2 Soft output based decoding of CCLC

For soft output based decoding of CCLC, we forward soft outputs to the interleaved LDPC code as follows. We start from the first column of $\mathbf{C}$ and for every symbol $c_{i,1} \in \underline{c}_1$, we compute the soft output

$$p(c_{i,1} = m | y_{i,1}^{i,L'}) \propto \sum_{x_{i,1}^{i,L'} | c_{i,1}=m} \frac{1}{\pi\sigma^2} e^{\frac{-\sum_{j=1}^{L'} \|y_{i,j} - x_{i,j}\|^2}{\sigma^2}} \tag{5.12}$$

for every $m \in \mathcal{M}$ where L' denotes a chosen depth. We then forward the soft outputs to a message passing decoder and decode $\underline{c}_1$. Under the assumption that

the SNR is higher than the BP threshold of the LDPC code, $\underline{c}_1$ can decoded with very high probability and thus assumed to be perfectly known. Similar to hard decision based decoding of CCLC, we repeat this procedure for the second column $\underline{c}_2$, under the assumption that the the first column is known, i.e. we compute $p(c_{i,2} = m|y_{i,2}^{i,1+L'}, c_{i,1})$ for $i \in \{1, \cdots, N_2\}$ and $m \in \mathcal{M}$. The remaining steps for soft output based decoding of CCLC are identical to hard decision based decoding. The encoding and decoding of CCLC is summarized in Fig. 5.2.

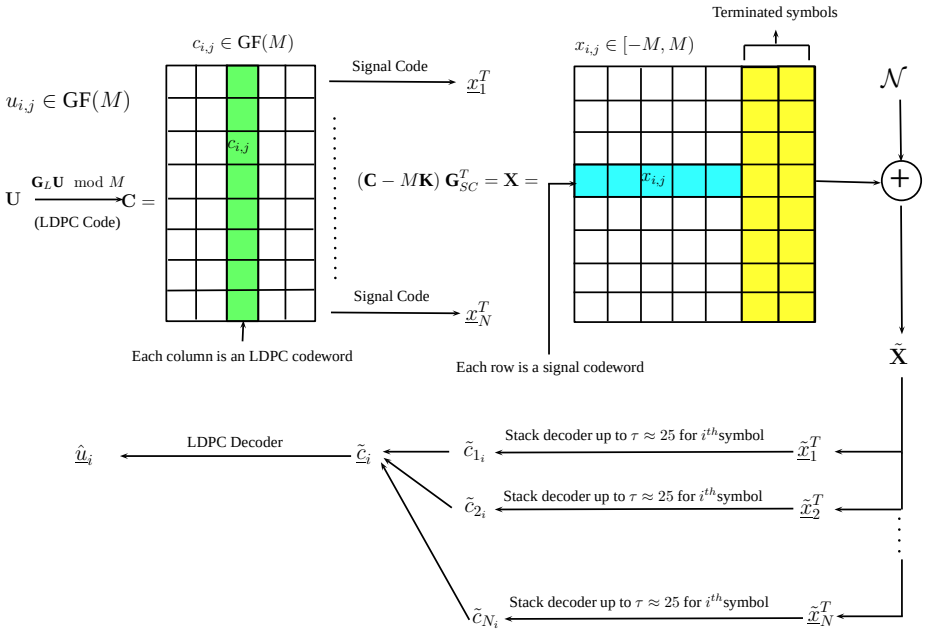

Figure 5.2: Encoding and decoding of CCLC

5.3.4 Achievable information rates with CCLC

Recall that $c_{i,j} \in \mathbb{F}_{M^2}$ are a sequence of coded symbols which are mapped to an M^2-QAM constellation denoted as $\mathcal{M}$. Under the assumption that the distribution on $c_{i,j}$ is independent and identically distributed (i.i.d) and uniform over $\mathbb{F}_{M^2}$ and

$N_1 \to \infty$, we denote the achievable information rate for each row $\mathbf{C}^i$ as $C_{i.i.d}$, which is given by

$$C_{i.i.d} = \frac{1}{N_2} I\left(\underline{C}^i; \underline{Y}^i | p(\underline{c}^i) = \prod_{j=1}^{N_2} p(c_{i,j})\right). \tag{5.13}$$

Due to hypercube shaping $C_{i.i.d} = I(X;Y)$, where X is a complex random variable with $\Re(X), \Im(X)$ uniformly distributed between $[-M, M)$ and $Y = X + Z$, where Z $\mathbb{C}\mathcal{N}(0, \sigma^2)$.

Using soft output based decoding of CCLC, the following propositions can be stated.

Proposition 29. *The equivalent channel across each column $\underline{c}_j$ is a memoryless channel.*

Proof. Each row of $\mathbf{C}$ is encoded independently from each other. Hence, the result follows. □

Proposition 30. *There are a finite number of statistically equivalent channels with posterior probability $\underline{p}\left(c_{i,j} | y_{i,j}^{i,j+L'}, c_{i,1}^{i,j-1}\right)$*

Proof. Due to hypercube shaping, the equivalent channel $\underline{p}\left(c_{i,j} | y_{i,j}^{i,j+L'}, c_{i,1}^{i,j-1}\right)$ depends on all of the past symbols $c_{i,1}^{i,j-1}$ as seen in (5.1), (5.2) and (5.3). The M^2 values $x_{i,j}$ can take with the assumption that $c_{i,1}^{i,j-1}$ is known, is shifted and folded on to $[-M, M)$. Note that the amount of the shift depends on $c_{i,1}^{i,j-1}$. As $N_2 \to \infty$, $x_{i,j}$ is uniformly distributed between $[-M, M)$ and thus there are uncountably infinite values it can take. Nonetheless, since each shift that results in the same ordering of the M^2 values after the folding operation would result in statistically identical channels, there would be only a finite number of equivalent channels with different

statistical properties. Due to the uniform distribution of $x_{i,j}$ in $[-M, M)$, each of the channels with different statistical properties are equally likely. □

Corollary 31. *For every $c_{i,j}$, the soft output ergodic mutual information, which we denote as I_S, can be computed as*

$$I_S = \frac{1}{\mathcal{S}} \sum_{s \in \mathcal{S}} I_s(C_{i,j}; Y_{i,j}^{i,j+L'} | C_{i,1}^{i,j-1}), \tag{5.14}$$

where $\mathcal{S}$ denotes the set of statistically different equivalent channels and I_s denotes the mutual information of a particular equivalent channel s.

Corollary 32. *The ergodic mutual information I_S gives a lower bound on $C_{i.i.d}$.*

Proof.

$$\frac{1}{N_2} \sum_{j=1}^{N_2} I(C_{i,j}; \underline{Y}^i | C_{i,1}^{i,j-1}) \geq I(C_{i,j}; Y_{i,j}^{i,j+L'} | C_{i,1}^{i,j-1}) \tag{5.15}$$

which follows from the data processing inequality since $Y_{i,j}^{i,j+L'}$ is a deterministic function of $\underline{Y}^i$. □

Corollary 33. *Using soft decision based decoding, the information rate I_S can be achieved if the interleaved LDPC code $\mathcal{C}$ achieves capacity.*

The ergodic mutual information for hard decision based decoding can be derived similarly, which we denote as I_H.

5.3.5 Simulation results

In this section, we shall demonstrate the performance of CCLC with hard decision based decoding and soft output based decoding. A filter pattern of $F(z) =$

$(1 + 0.98e^{j0.09\pi}z^{-1})^3$, which was shown to be a monic causal filter with good minimum distance properties in [13], is used for encoding the LDPC codeword matrix $\mathbf{C}$ to the signal codeword matrix $\mathbf{X}$. Due to hypercube shaping, $x_{i,j}$ is uniformly distributed between $\big[-M, M\big)$ as $N_2 \to \infty$. Therefore, $E(|x_{i,j}|^2) = \frac{M^2}{6}$ and SNR is defined as $SNR = \frac{E(|x_{i,j}|^2)}{2\sigma^2}$ where σ^2 is the variance of real and imaginary components of complex AWGN and hence $SNR = \frac{M^2}{12\sigma^2}$. Since I_S and I_H denote ergodic mutual information, we estimate them by averaging over 10^5 $c_{i,j}$'s with known past symbols. We choose N_1, in other words the LDPC codeword length to be 10^6. The LDPC codes were constructed over $GF(M^2)$ a uniform weight distribution for edges with degree distributions of $(3, k)$ where $k \in \{6, 9, 12, 15, 30\}$ which results in code rates $\frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{9}{10}\}$, respectively. For hard decision based decoding, simulations were carried out for 9-QAM and 25-QAM constellations and a stack decoder with size 1000 was used with a depth of $\tau = 25$. For soft output based decoding, a 16-QAM constellation was used with $L' = L + 1 = 4$. Since the LDPC codes are chosen over non-binary fields, the thresholds were estimated empirically by determining the minimum SNR where 10 codewords were decoded correctly consecutively.

As seen in Fig. 5.3, 5.4 and 5.5, I_S approaches $C_{i.i.d}$ much closer than I_H even though the depth of the soft output based decoder L' is much smaller than the depth of the hard decision based decoder τ. This can be attributed to the fact that the soft outputs can be computed exactly for a depth L' and the only suboptimality arises from L' being less than N_2. On the other hand, the suboptimality of the hard decision based decoder arises from both the stack decoder being suboptimal and τ being less than N_2. Furthermore, there is also the inherent advantage of a soft outputs channel having a larger capacity over a hard decision channel. For both hard decision based decoding and soft output based decoding, it can be observed that the LDPC thresholds are within 1 dB from I_H and I_S, respectively.

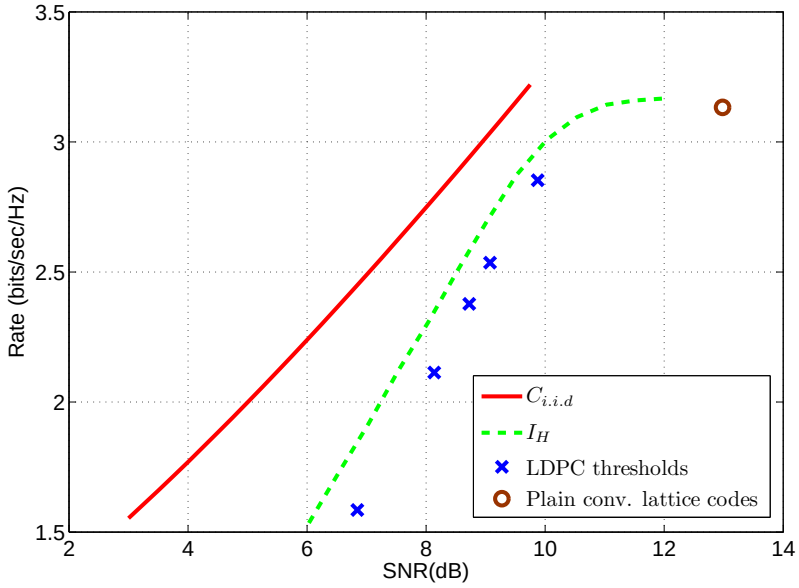

Figure 5.3: Performace of CCLC over 9-QAM with hard decision decoding

5.4 Extension to compute-and-forward

5.4.1 System model

In Fig. 5.6, we depict the bidirectional relay network, where there are two source nodes, which we denote as S_1 and S_2, that would like to exchange information with each other. These source nodes do not have a direct path of communication, but they are able to communicate through a relay, which we denote as R. The relay is able to receive from and transmit to both nodes, via a multiple access channel (MAC) and broadcast channel, respectively. S_1 and S_2 encode their information matrices $\mathbf{U}_1, \mathbf{U}_2 \in \mathbb{F}_{M^2}^{k \times N_2}$, respectively, to codewords $\mathbf{X}_1, \mathbf{X}_2 \in \mathbb{C}^{N_1 \times N_2}$, respectively, and transmit during the MAC phase. Under the assumption that channel gains are

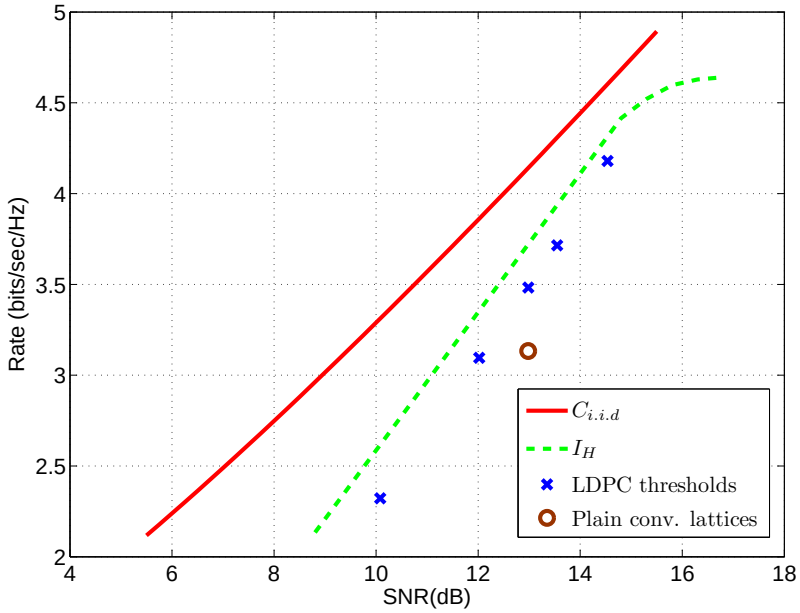

Figure 5.4: Performace of CCLC over 25-QAM with hard decision decoding

unit and there is perfect synchronization, the relay observes

$$\mathbf{Y}_R = \mathbf{X}_1 + \mathbf{X}_2 + \mathbf{Z} \tag{5.16}$$

where each $z_{i,j} \sim \mathbb{C}\mathcal{N}(0, \sigma^2)$ and i.i.d. The relay then decodes to a function $f(\mathbf{C}_1, \mathbf{C}_2)$ and broadcasts it to the transmitters during the broadcast phase. $f(\mathbf{U}_1, \mathbf{U}_2)$ is chosen specifically such that upon receiving it, each transmitter can determine the other transmitter's information matrix with the knowledge of its own information vector.

5.4.2 CCLC for compute-and-forward

5.4.2.1 Encoding for the MAC phase

We choose our function to be decoded at the relay as $f(\mathbf{C}_1, \mathbf{C}_2) = \mathbf{C}_1 \oplus \mathbf{C}_2$. In order to decode to this function, encoding at the transmitters are done slightly

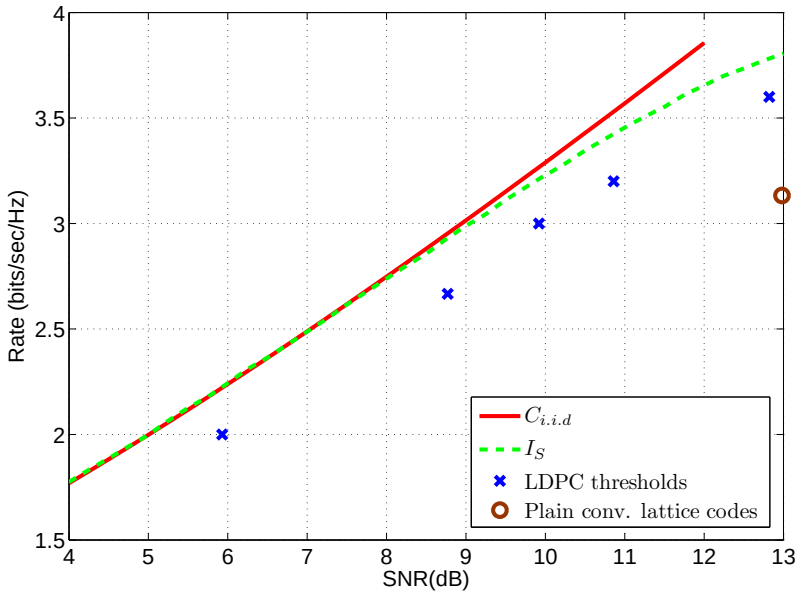

Figure 5.5: Performace of CCLC over 16-QAM with soft decision decoding

different from the point-to-point case as follows. For each transmitter $l \in \{1, 2\}$, the information matrix $\mathbf{U}_l$ are divided into real and imaginary parts, i.e., $\Re(\mathbf{U}_l), \Im(\mathbf{U}_l) \in \mathbb{F}_M^{K \times N_2}$ rather than $\mathbf{U}_l \in \mathbb{F}_{M^2}^{K \times N_2}$ as in the point-to-point case. Each column $\Re(\underline{u_l})^j$, $\Im(\underline{u_l})^j$ are then encoded to $\Re(\underline{c_l})^j$ and $\Im(\underline{c_l})^j$, respectively via an LDPC code $\mathcal{C}$ over $\mathbb{F}_M$ with rate $R = \frac{K}{N_1}$. Each element of $\Re(\mathbf{C}_l)$ and $\Im(\mathbf{C}_l)$ are then mapped to the M^2-QAM constellation $\mathcal{M}$ as $\mathbf{A}_l = t(\Re(\mathbf{C}_l)) + jt(\Im(\mathbf{C}_l))$, where $t(\dot{})$ denotes the trivial mapping from $\mathbb{F}_M$ to $\mathbb{Z}$. For notational convenience, we shall drop $t(\dot{})$. The remaining steps for encoding $\mathbf{X}_1$ and $\mathbf{X}_2$ are identical to what was described in Sec. 5.3.2.

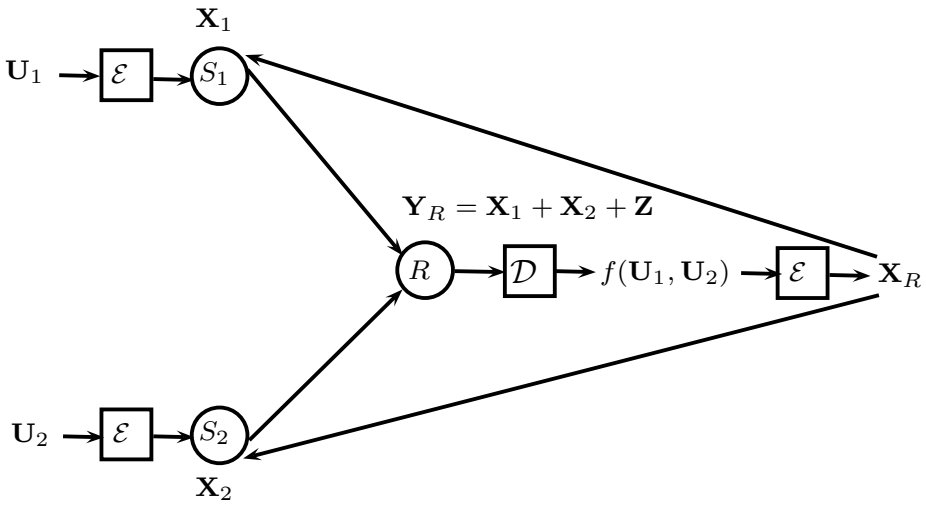

Figure 5.6: Compute-and-forward for the bidirectional relay network

5.4.2.2 Decoding at the relay

During the MAC phase, the relay observes

$$\mathbf{Y}_R = \mathbf{X}_1 + \mathbf{X}_2 + \mathbf{Z} \tag{5.17}$$

and it will attempt to decode to $\Re(\mathbf{C}_1) \oplus \Re(\mathbf{C}_2)$ and $\Im(\mathbf{C}_1) \oplus \Im(\mathbf{C}_2)$. Let $\tilde{\mathbf{X}} = \mathbf{X}_1 + \mathbf{X}_2$. Note that $\tilde{\mathbf{X}}$ can be written as,

$$\begin{aligned}
\tilde{\mathbf{X}} &= (\mathbf{A}_1 - M\mathbf{K}_1)\,\mathbf{G}_{CL}^T + (\mathbf{A}_2 - M\mathbf{K}_2)\,\mathbf{G}_{CL}^T \\
&= (\mathbf{A}_1 + \mathbf{A}_2 - M\,(\mathbf{K}_1 + \mathbf{K}_2))\,\mathbf{G}_{CL}^T \\
&= (\Re(\mathbf{C}_1) + \Re(\mathbf{C}_2) + j\,(\Im(\mathbf{C}_1) + \Im(\mathbf{C}_2)) \\
&\quad - M\,(\mathbf{K}_1 + \mathbf{K}_2))\mathbf{G}_{CL}^T \\
&= (\Re(\tilde{\mathbf{C}}) + j\Im(\tilde{\mathbf{C}}) - M\tilde{\mathbf{K}})\mathbf{G}_{CL}^T
\end{aligned} \tag{5.18}$$

where $\Re(\tilde{\mathbf{C}}) = \Re(\tilde{\mathbf{C}}_1) \oplus \Re(\tilde{\mathbf{C}}_2)$, $\Im(\tilde{\mathbf{C}}) = \Im(\tilde{\mathbf{C}}_1) \oplus \Im(\tilde{\mathbf{C}}_2)$ and

$$\begin{aligned}\tilde{\mathbf{K}} = \mathbf{K}_1 + \mathbf{K}_2 + \frac{\Re(\mathbf{C}_1) + \Re(\mathbf{C}_2) - (\Re(\mathbf{C}_1) \oplus \Re(\mathbf{C}_2))}{M} \\ + j\frac{\Im(\mathbf{C}_1) + \Im(\mathbf{C}_2) - (\Im(\mathbf{C}_1) \oplus \Im(\mathbf{C}_2))}{M}\end{aligned} \tag{5.19}$$

Comparing (5.10) to (5.18), the observation at the relay can be thought of as encoding $\tilde{C}$ to a CCLC codeword matrix $\tilde{X}$ with the only difference being $\Re(\tilde{x}_{i,j}), \Im(\tilde{x}_{i,j}) \in [-M, M)$ instead of $[-M/2, M/2)$ as in the point-to-point case. We would like to note that in the point-to-point case, for every $\mathbf{C}$, there is a unique Gaussian integer matrix $\mathbf{K}$ that satisfies the hypercube shaping constraint. However during the MAC phase due to the addition of $\mathbf{X}_1$ and $\mathbf{X}_2$, there are multiple $\tilde{\mathbf{K}}$'s for every $\tilde{\mathbf{C}}$ that result in $\Re(\tilde{x}_{i,j}), \Im(\tilde{x}_{i,j}) \in [-M, M)$. More specifically, given $\underline{\tilde{c}}_{i,1}^{i,j-1}$ and $\underline{\tilde{k}}_{i,1}^{1,j-1}$, there are exactly four $\tilde{k}_{i,j}$'s for each M^2 candidate of $\tilde{c}_{i,j}$ that result in $\Re(\tilde{x}_{i,j}), \Im(\tilde{x}_{i,j}) \in [-M, M)$.

It can be observed from the statistical properties of the noise that among the four $\tilde{k}_{i,j}$'s for every candidate of $\tilde{c}_{i,j}$, only one of them is likely to have been subtracted due to the following. The four $\tilde{k}_{i,j}$'s are placed as a shifted 4-QAM constellation which has a minimum distance of 1. Taking into account that these $\tilde{k}_{i,j}$'s are multiplied my M as seen in (5.18) and achieving a certain rate with hypercube requires an additional 1.53 dB loss compared to the AWGN channel capacity, the probability that the magnitude of the noise element $z_{i,j}$ exceeds $M/2$ can be computed as

$$\begin{aligned}p(\|z_{i,j}\| > \frac{M}{2}) &= e^{-\frac{M^2}{4\sigma^2}} \\ &= e^{-2.133(M^{2R}-1)}.\end{aligned} \tag{5.20}$$

where R is the coding rate of the LDPC code.

As seen in (5.20), $p(|z_{i,j}| > \frac{M}{2})$ is quite small for a fixed R if M is large. For

example if $M = 7$ and $R = 0.7$, $p(\|z_{i,j}\| > \frac{M}{2}) \approx 10^{-13}$. Note that the events $\|z_{i,j}\| > \frac{M}{2}$ and $\tilde{x}_{i,j} \notin \mathcal{B}(\tilde{y}_{i,j}, M/2)$ are identical. Therefore for both hard decision based decoding and soft output based decoding of CCLC, out of the four $\tilde{k}_{i,j}$'s for each candidate of $\tilde{c}_{i,j} \in \mathbb{F}_M^2$, we pick the one that results in $\tilde{x}_{i,j} \in \mathcal{B}(\tilde{y}_{i,j}, M/2)$ since it is quite unlikely that any of the other $\tilde{k}_{i,j}$'s were subtracted. Also, due to the fact that $\tilde{k}_{i,j}$'s form a 4-QAM constellation with a minimum distance of 1, it is not possible for multiple $\tilde{k}_{i,j}$'s to result in $\tilde{x}_{i,j} \in \mathcal{B}(\tilde{y}_{i,j}, M/2)$ for a given $\tilde{c}_{i,j}$. Furthermore, there is also a possibility that none of the $\tilde{k}_{i,j}$'s result in $\tilde{x}_{i,j} \in \mathcal{B}(\tilde{y}_{i,j}, M/2)$ for a given $\tilde{c}_{i,j} = \tilde{c}$ where $\tilde{c} \in \mathbb{F}_M^2$, which in this case we simply assume that $p(\tilde{c}_{i,j} = \tilde{c}|\mathbf{Y}, \underline{\tilde{c}}_{i,1}^{i,j-1}, \underline{\tilde{k}}_{i,1}^{i,j-1}) = 0$. With these assumptions, there is no ambiguity in the $\tilde{k}_{i,j}$'s and we can proceed with either hard decision based decoding or soft output based decoding as described in Sec. 5.3.3.

Once $\Re(\tilde{\mathbf{C}}) = \Re(\mathbf{C}_1) \oplus \Re(\mathbf{C}_2)$ and $\Im(\tilde{\mathbf{C}}) = \Im(\mathbf{C}_1) \oplus \Im(\mathbf{C}_2)$ is recovered at the relay, it can be re-encoded as described in Sec. 5.4.2.1 and broadcasted to both transmitters. Assuming that the transmitters are able to decode to $\Re(\tilde{\mathbf{C}}) = \Re(\mathbf{C}_1) \oplus \Re(\mathbf{C}_2)$ and $\Im(\tilde{\mathbf{C}}) = \Im(\mathbf{C}_1) \oplus \Im(\mathbf{C}_2)$, they can recover each other's information by subtracting their own. We would like to note that the broadcast channel can be thought of as two parallel point-to-point AWGN channels and hence the achievable rate is identical to the point-to-point case. However, the same assumption can not be made for the MAC channel and we compute the ergodic mutual information for hard decision based decoding and soft output based decoding as we did in Sec. 5.3.4, which we denote as I_H and I_S, respectively, in the following section.

5.4.3 Simulation results

In this section, we demonstrate the performance of CCLC with hard decision based decoding and soft output based decoding for compute-and-forward over the

bidirectional relay network. We choose the same filter pattern as in Sec. 5.3.5 for encoding CCLC at the transmitters and at the relay. In order to ensure $p(\|z_{i,j}\| > M/2)$ is sufficiently small, we choose $M = 7$ and the degree distributions of the regular LDPC codes as $(3, k)$ for $k \in \{6, 9, 12, 15, 30\}$ which result in code rates of $\{\frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{9}{10}\}$, respectively as in Sec. 5.3.5. We choose the LDPC codes to be over $\mathbb{F}_7$ in order to encode the real and imaginary components of $\mathbf{U}_1$ and $\mathbf{U}_2$ separately. For hard decision based decoding, we choose a depth of $\tau = 25$ and a stack size of 1000, whereas for soft decision based decoding we choose $L' = 4$ as in Sec. 5.3.5.

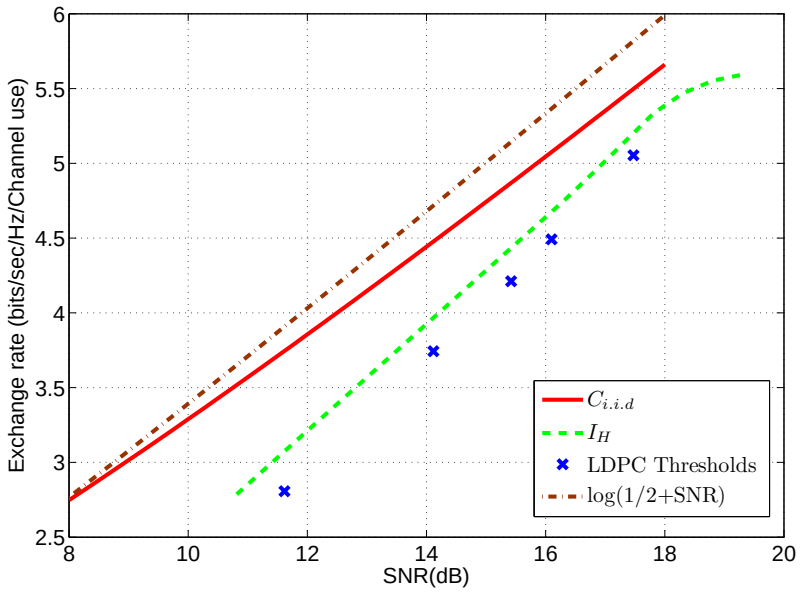

Figure 5.7: Performace of CCLC over 49-QAM with hard decision decoding

As seen in Fig. 5.7 and 5.8, when CCLC is used for compute-and-forward, there is a negligible loss in the SNR required to achieve same exchange rate/channel use as in the point-to-point case. This can be attributed to the fact that each row in

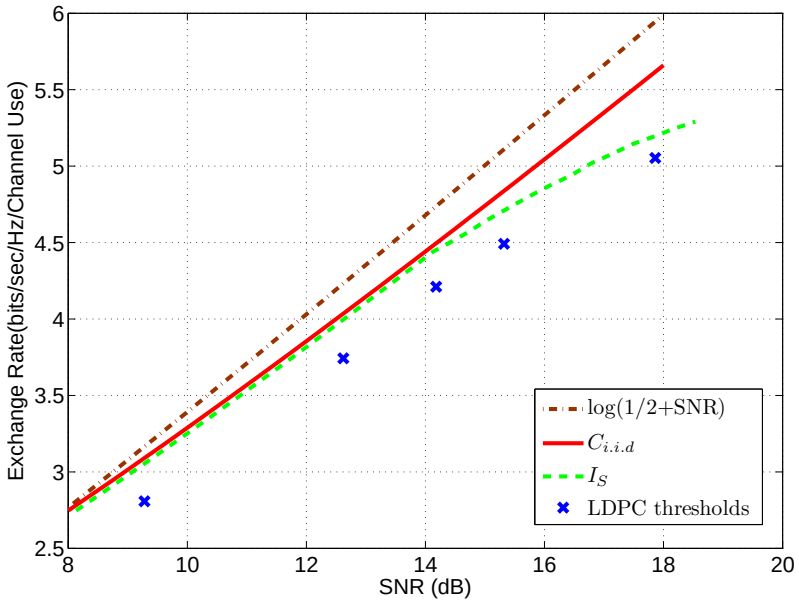

Figure 5.8: Performace of CCLC over 49-QAM with soft decision decoding

$\mathbf{X}_1$ and $\mathbf{X}_2$ belong to the same lattice and hence each row of $\tilde{\mathbf{X}} = \mathbf{X}_1 + \mathbf{X}_2$ also belongs to the same lattice due to lattices being closed under addition. Furthermore, the ambiguity of multiple $\tilde{k}_{i,j}$'s are resolved due to our assumption in Sec. 5.4.2.2. Thus, a very similar performance to the point-to-point case can be obtained when decoding at the relay. It can also be observed from Fig. 5.8 that the exchange rate using the soft output based decoder is to within 1.7 dB from $\log(1/2 + SNR)$, which was shown to be an achievable rate by using nested lattice codes, and most of this gap is a direct consequence of using hypercube shaping at the transmitters and thus losing 1.53 dB.

5.5 Conclusion and further improvements

A new lattice-based coding scheme has been introduced based on concatenating convolutional lattice codes with interleaved LDPC codes. The structure of these

codes enable them to achieve good asymptotic performance in block length while allowing the stack size to be small. Furthermore, simulation results show that they can approach capacity very closely. The algebraic structure of these codes make them a good candidate for implementing compute-and-forward, which simulation results show that they can approach the theoretically achievable rates to within 1.7 dB. For future work, other shaping algorithms can be developed in order to further bridge this gap. Also, the performance of CCLC can be observed in a more general network setup such as an AWGN network which consists of K transmitters and M relays with non-unit channel gains.

6. CONCLUSION

In this dissertation, we extended Nazer and Gastpar's lattice-based compute-and-forward framework to recovering Eisenstein integer linear combinations of transmitted messages. Our main motivation lied under the fact that that since channel coefficients are in some sense approximated by integers and Eisenstein integers quantize the complex field better than Gaussian integers, on average higher computation rates would be achievable. In order to extend this framework to lattices over Eisenstein integers, we first proved the existence of lattices over Eisenstein integers that are simultaneously good for quantization and good for AWGN channel coding. Then, we derived the achievable computation rates of this extended framework, which simulation results showed a 0.4 dB improvement in outage performance over decoding to Gaussian integer linear combinations.

We then introduced a separation-based framework for compute-and-forward that employs linear codes over Eisenstein lattice partitions. Our motivation in designing this framework was to develop a practically implementable framework and investigate whether it would be possible to diminish the effect of channel quantization and achieve higher rates than the lattice-based framework. We derived the achievable rates of this separation-based framework and showed that it is possible to achieve higher rates than the lattice-based framework.

In the second part of this dissertation, we built spatially-coupled LDA lattices from spatially-coupled LDPC codes and showed that these lattices closely approach the Poltyrev limit for the point-to-point unconstrained AWGN channel. Motivated by this result, we employed these lattices to build spatially-coupled LDA lattice codes for our separation-based framework. Simulation results show that spatially-coupled

LDA lattice codes can closely approach approach the theoretically achievable rates for the separation-based framework

In the last part of this dissertation, we introduced a new class of lattice codes which we refer to as concatenated convolutional lattice codes (CCLC). These codes comprise of convolutional lattice codes which are interleaved with LDPC codes. Our main motivation was to enhance the error correcting capability of convolutional lattice codes and reduce their decoding complexity. We designed a hard-decision and soft-decision based decoding scheme and simulated CCLC for the point-to-point AWGN channel. Simulation results showed that with soft-decision based decoding, CCLC can approach capacity as close as 0.1dB. Motivated by these results, we employed CCLC for implementing the compute-and-forward paradigm in a bidirectional relay network. For this setup, simulation results showed that CCLC can closely approach $\log(1/2 + SNR)$, which is the achievable rate of employing nested lattice codes for compute-and-forward, as close as 0.5 dB.

REFERENCES

[1] S. Lin and D. J. Costello, *Error Control Coding*, 2nd ed., Pearson Prentice Hall, New Jersey, 2004.

[2] T. Li and O. M. Collins, "A Successive Decoding Strategy for Channels with Memory," *IEEE Trans. Info. Theory*, vol. 53, no. 2, pp. 628-646, 2007.

[3] K. R. Narayanan and N. Nangare, "A BCJR-DFE Based Receiver for Achieving Near Capacity Performance on Inter Symbol Interference Channels," *Proceedings 42nd Allerton Conference on Communications*, Oct. 2004.

[4] J. B. Soriaga, H. D. Pfister, and P. H. Siegel, "Determining and Approaching Achievable Rates of Binary Intersymbol Interference Channels using Multistage decoding," *IEEE Trans. Info. Theory,* vol. 53, no. 4, pp. 1416-1429, 2007.

[5] H. D. Pfister, J. B. Soriaga, and P. H. Siegel, "On the Achievable Information Rates of Finite State ISI Channels," *IEEE Global Telecommunications Conference*, pp. 2992-2996, 2001.

[6] B. Nazer and M. Gastpar, "Compute-and-Forward: Harnessing Interference through Structured Codes," *IEEE Trans. Info. Theory*, vol. 57, no. 10, pp. 6463-6486, Oct. 2011.

[7] C. Feng, D. Silva, and F. R. Kschischang, "An Algebraic Approach to Physical-Layer Network Coding," *IEEE Intl. Symp. on Info. Theory*, pp. 1017-1021, Jun. 2010.

[8] U. Erez, S. Litsyn, and R. Zamir, "Lattices which are Good for (Almost) Everything," *IEEE Trans. Info. Theory*, vol. 51, no.10, pp. 3401-3416, Oct. 2005.

[9] U. Erez and R. Zamir, "Achieving 1/2 log (1+ SNR) on the AWGN Channel with Lattice Encoding and Decoding," *IEEE Trans. Info. Theory*, vol. 50, no. 10, pp. 2293-2314, Oct. 2004.

[10] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices, and Groups*, 3rd ed., Springer-Verlag, New Jersey, 1999.

[11] R. Zamir and M. Feder, "On lattice quantization noise," *IEEE Trans. Info. Theory*, pp. 1152-1159, vol. 42, no. 4, Jul. 1996.

[12] N. Sommer, M. Feder, and O. Shalvi, "Low Density Lattice Codes," *IEEE Trans. Info. Theory*, vol. 54, no. 4, pp. 1561-1585, Apr. 2008.

[13] O. Shalvi, N. Sommer, and M. Feder, "Signal Codes," *Information Theory Workshop*, pp. 332-336, 2003.

[14] R. Breusch, "Zur Verallgemeinerung des Bertrandsehen Postulates, daß Zwischen x und 2x Stets Primzalflen Liegen," *Mathematische Zeitschrift*, vol. 34, no.1, pp. 505-526, 1932.

[15] H. A. Loeliger, "Averaging Bounds for Lattices and Linear Codes," *IEEE Trans. Info. Theory*, vol. 43, no. 5, pp. 1767-1773, Nov. 1997.

[16] J. H. Conway and D. Smith, *On Quaternions and Octonions: Their Geometry, Arithmetic, and Symmetry*, AK Peters, Massachusetts, 2003.

[17] G. D. Forney Jr., "Coset Codes. I. Introduction and Geometrical Classification," *IEEE Trans. Info. Theory*, vol. 34, no. 5, pp. 1123-1151, Sep. 1998.

[18] G. Poltyrev, "On Coding without Restrictions for the AWGN Channel," *IEEE Trans. Info. Theory*, vol. 40, no. 2, pp. 409-417, Mar. 1994.

[19] C. A. Rogers, "A Note on Coverings," *Mathematica*, vol. 4, pp. 1-6, 1957.

[20] M. Tomlinson, "New Automatic Equalizer Employing Modulo Arithmetic," *Electronics Letters*, vol. 7, no. 5, pp. 138-139, Mar. 1971.

[21] O. Shalvi, N. Sommer, and M. Feder, "Signal Codes: Convolutional Lattice Codes," *IEEE Trans. Info. Theory*, vol. 57, no. 8, pp. 5203-5226, Aug. 2011.

[22] S. Kudekar, T. Richardson, and R. Urbanke, "Threshold Saturation via Spatial Coupling: Why Convolutional LDPC Ensembles Perform so Well over the BEC," *IEEE Trans. Info. Theory*, vol. 57, no. 2, pp. 803-834, Feb. 2011.

[23] S. Kudekar, T. Richardson, and R. Urbanke, "Spatially Coupled Ensembles Universally Achieve Capacity under Belief Propagation," *www.arxiv.org*, Jan. 2012.

[24] M. P. Wilson, K. R. Narayanan, H. D. Pfister, and A. Sprintson, "Joint Physical Layer Coding and Network Coding for Bi-Directional Relaying," *IEEE Trans. Info. Theory*, vol. 56, no. 11, pp. 5641-5654, Nov. 2010.

[25] W. Nam, S. Y. Chung, and Y. H. Lee, "Capacity of the Gaussian Two-Way Relay Channel to within 1/2 Bit," *IEEE Trans. Info. Theory*, vol. 56, no. 11, pp. 5488-5494, Nov. 2010.

[26] N. di Pietro, J. J. Boutros, G. Zemor, and L. Brunel, "Integer Low-Density Lattices based on Construction A," *Information Theory Workshop*, Lausanne, Switzerland, Sep. 2012.

[27] N. di Pietro, J. J. Boutros, G. Zemor, and L. Brunel, "New Results on Low-Density Integer Lattices," *Information Theory and Applications Workshop*, San Diego, CA, Feb. 2013.

[28] N. E. Tunali, K. R. Narayanan, J. J. Boutros, and Y.-C. Huang, "Lattices over Eisenstein Integers for Compute and Forward," *Proceedings 50th Annual Allerton Conference on Communications*, pp. 33-40, Monticello, IL, Oct. 2012.

[29] R. Zamir, S. Shamai, and U. Erez,"Nested Linear/Lattice Codes for Structured Multiterminal Binning," *IEEE Trans. Info. Theory*, vol. 48, no.6, pp. 1250-1276, Jun. 2002.

[30] B. M. Kurkoski and J. Dauwels, "Message-Passing Decoding of Lattices Using Gaussian Mixtures," *IEEE Intl. Symp. on Info. Theory*, pp. 2489-2493, Jul. 2008.

[31] Y. Yan, C. Ling, and X. Wu, " Polar Lattices: Where Arikan Meets Forney," *IEEE Intl. Symp. on Info. Theory*, pp. 1292-1296, Jul. 2013.

[32] J. H. Conway and N. J. A. Sloane, "A Fast Encoding Method for Lattice Codes and Quantizers," *IEEE Trans. Info. Theory*, vol. 39, no. 6, pp. 820-824, Nov. 1983.

[33] J. Leech and N. J. A. Sloane, "Sphere Packings and Error Correcting Codes," *Canadian Journal of Mathematics*, vol. 23, no. 4, pp. 718-745, Nov. 1971.

[34] T. W. Hungerford, *Algebra (Graduate Texts in Mathematics)*, Springer-Verlag, New York, 1974.

[35] T. Richardson and R. Urbanke, *Modern Coding Theory*, Cambridge University Press, New York, 2008.

[36] O. Ordentlich and U. Erez, "A Simple Proof for the Existence of "Good" Pairs of Nested Lattices," *IEEE Convention of Electrical Engineers in Israel*, Nov. 2012.

[37] U. Niesen and P. Whiting, "The Degrees of Freedom of Compute-and-Forward," *IEEE Trans. Info. Theory*, vol. 58, no. 8, pp. 5214-5232, Aug. 2012.

[38] H. Uchikawa, B. M. Kurkoski, K. Kasai, and K. Sakaniwa, "Threshold Improvement of Low-Density Lattice Codes via Spatial Coupling," *Proceedings International Conference on Computing, Networking, and Communications*, pp. 1036-1040, 2012.

[39] N. E. Tunali, K. R. Narayanan, and H. D. Pfister, "Spatially-Coupled Low Density Lattices Based on Construction A with Applications to Compute-and-Forward," *Information Theory Workshop*, pp. 1-5, Sep. 2013.

[40] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative Diversity in Wireless Networks: Efficient Protocols and Outage Behaviour," *IEEE Trans. Info. Theory*, vol. 50, pp. 3062-3080, Dec. 2004.

[41] T. M. Cover and A. El Gamal, "Capacity Theorems for the Relay Channel," *IEEE Trans. Info. Theory*, vol. 25, pp. 572-584, Sept. 1972

APPENDIX A

APPENDIX TO CHAPTER 3

In this appendix, we provide the proof for Theorem 22.

A.1 Proof of the existence of good nested $\mathbb{Z}[\omega]$-lattices

Using our result from Theorem 19, let Λ be an n-dimensional $\mathbb{Z}[\omega]$-lattice obtained through Construction-A with a corresponding generator matrix $\mathbf{B}$ which is good for covering.

Definition 34. *A set $\mathcal{C}$ of linear (n,k) linear code over $\mathbb{F}_q^n$ is* balanced *if every nonzero element of $\mathbb{F}_q^n$ is contained in the same number, denoted by $N_{\mathcal{C}}$ of codes from $\mathcal{C}$.*

Note that for fixed n, k, and q, the set of all linear (n,k) codes over $\mathbb{F}_q$ is balanced. We shall now state Lemma 1 in [15].

Lemma 35. *Let $f(\cdot)$ be an arbitrary mapping $\mathbb{F}_q^n \to \mathbb{R}$ and let $\mathcal{C}$ be a balanced set of linear (n,k) codes over $\mathbb{F}_q$. Then, the average over all linear codes C in $\mathcal{C}$ of the sum $\sum_{c\in C'} f(c)$ is given by*

$$\frac{1}{\mathcal{C}}\sum_{C\in\mathcal{C}}\sum_{c\in C'} f(c) = \frac{q^k-1}{q^n-1}\sum_{v\in\left(\mathbb{F}_q^n\right)'} f(v) \tag{A.1}$$

For proving Theorem 22, we shall use nested $\mathbb{Z}[\omega]$-lattices obtained from Construction-A as mentioned in section 3.2.3. A scaled version of Λ_C denoted as $\gamma\Lambda_C$, where $\gamma \in \mathbb{R}^+$ and Λ_C was defined in section 3.2.2 is constructed. Then, we multiply $\gamma\Lambda_C$ with the generator matrix $\mathbf{B}$ and obtain the lattice $\Lambda_f = \gamma\mathbf{B}\Lambda_C$. It can be observed

that $\gamma\varrho\mathbb{Z}[\omega]^n \subset \gamma\varrho\Lambda \subset \Lambda_f$ and there are q^k elements of Λ_f that lie within the fundamental Voronoi region of $\gamma\varrho\Lambda$. Hence, the volume of the fundamental region of Λ_f is

$$\mathrm{Vol}\left(\mathcal{V}_{\Lambda_f}\right) = \gamma^{2n} q^{n-k} \left(\frac{\sqrt{3}}{2}\right)^n \mathrm{Vol}\left(\mathcal{V}_{\Lambda}\right). \tag{A.2}$$

We can now extend the Minkowski-Hlawka Theorem in [15] to Eisenstein lattices as follows, following similar steps.

Theorem 36. *(*Minkowski-Hlawka Theorem:*) Let f be a Riemann integrable function $\mathbb{R}^{2n} \to \mathbb{R}$ of bounded support(i.e., $f(v) = 0$ (if $\|v\|$ exceeds some bound). Then for any integer k where $0 < k < n$, and any fixed $Vol(\mathcal{V}_{\Lambda_f})$, the approximation*

$$\frac{1}{\mathcal{C}} \sum_{C \in \mathcal{C}} \sum_{v \in g(\gamma \mathbf{B} \Lambda'_C)} f(v) \approx Vol(\mathcal{V}_{\Lambda_f})^{-1} \int_{\mathbb{R}^{2n}} f(v) dv \tag{A.3}$$

where $\mathcal{C}$ is any balanced set of linear (n,k) codes over $\mathbb{F}_q$ and where $g(\cdot) : \mathbb{C}^n \to \mathbb{R}^{2n}$ as in (3.6)*, becomes exact in the limit $q \to \infty$, $\gamma \to 0$, $\gamma^{2n} q^{n-k} \left(\frac{\sqrt{3}}{2}\right)^n Vol\left(\mathcal{V}_{\Lambda}\right) = Vol\left(\mathcal{V}_{\Lambda_f}\right)$ fixed. Note that these conditions imply that $\gamma q \to \infty$.*

Proof.

$$\frac{1}{|\mathcal{C}|}\sum_{C\in\mathcal{C}}\sum_{v\in g(\gamma\mathbf{B}\Lambda'_C)} f(v) \tag{A.4}$$

$$= \frac{1}{|\mathcal{C}|}\sum_{C\in\mathcal{C}}\Big[\sum_{v\in g\left((\mathbb{Z}[\omega]^n)'\right):\tilde{\sigma}(v)=0} f(\gamma\mathbf{B}v)\dots$$

$$\dots + \sum_{v\in g(\mathbb{Z}[\omega]^n):\tilde{\sigma}(v)\in C'} f(\gamma\mathbf{B}v)\Big] \tag{A.5}$$

$$= \sum_{v\in\left(g(\mathbb{Z}[\omega]^n)'\right):\tilde{\sigma}(v)=0} f(\gamma\mathbf{B}v)$$

$$+ \frac{1}{|\mathcal{C}|}\sum_{C\in\mathcal{C}}\sum_{c\in\mathcal{C}'}\left[\sum_{v\in g(\mathbb{Z}[\omega]^n):\tilde{\sigma}(v)=c} f(\gamma\mathbf{B}v)\right] \tag{A.6}$$

$$= \sum_{v\in g\left((\mathbb{Z}[\omega]^n)'\right):\tilde{\sigma}(v)=0} f(\gamma\mathbf{B}v)$$

$$+ \frac{q^k-1}{q^n-1}\sum_{c\in(\mathbb{F}_q^n)'}\left[\sum_{v\in g(\mathbb{Z}[\omega]^n):\tilde{\sigma}(v)=c} f(\gamma\mathbf{B}v)\right] \tag{A.7}$$

$$= \sum_{v\in g\left((\mathbb{Z}[\omega]^n)'\right):\tilde{\sigma}(v)=0} f(\gamma\mathbf{B}v)$$

$$+ \frac{q^k-1}{q^n-1}\sum_{v\in g(\mathbb{Z}[\omega]^n):\tilde{\sigma}(v)\neq 0} f(\gamma\mathbf{B}v) \tag{A.8}$$

where the step from (A.6) to (A.7) is due to Lemma 35 and due to the fact that f has bounded support, the left term of (A.8) vanishes for sufficiently large γq and the

right term of (A.8) becomes

$$\frac{q^k-1}{q^n-1}\sum_{v\in g((\mathbb{Z}[\omega]^n)')} f(\gamma\mathbf{B}v) \approx \gamma^{-2n}q^{k-n}\left(\frac{2}{\sqrt{3}}\right)^n \mathrm{Vol}(\mathcal{V}_\Lambda)^{-1}\int_{\mathbb{R}^{2n}} f(v)dv \tag{A.9}$$

which becomes exact in the limit as $\gamma \to 0$, $\gamma q \to \infty$, i.e, a Riemann sum approaching to a Riemann integral. Note that the term $\gamma^{-2n}q^{k-n}\left(\frac{2}{\sqrt{3}}\right)^n$ appears in front of the integral in (A.9) since it is the reciprocal of the volume of the fundamental Voronoi region of $\Lambda_f = \gamma\mathbf{B}\Lambda_C$. □

Suppose now that a transmitter selects a codeword $\underline{x}$ from an Eisenstein lattice $\Lambda \in \mathbb{C}^n$ (or equivalently $\mathbb{R}^{2n}$) and $\underline{x}$ is transmitted over an AWGN channel where a random noise vector $\underline{z} \in \mathbb{C}^n$(or equivalently $\mathbb{R}^{2n}$) gets added with the variance of each $2n$ components equal to $P_{\underline{z}}/2$. The receiver obtains $\underline{y} = \underline{x} + \underline{z}$ and tries to recover $\underline{x}$. Furthermore, let $E \subset \mathbb{R}^{2n}$ be a set of typical noise vectors. We say that an *ambiguity* occurs if $\underline{y}$ can be written in more than one way as $\underline{y} = \underline{x} + \underline{e}$ where $\underline{x} \in \Lambda$ and $\underline{e} \in E$. Let $P_{\mathrm{amb}|E}$ be the probability of ambiguity given that $\underline{z} \in E$. Assuming that the receiver is able to recover $\underline{x}$ whenever $\underline{z} \in E$ and there is no ambiguity, the probability of decoding error is upper-bounded by

$$P_e \leq P_{\mathrm{amb}|E} + P(\underline{z} \notin E) \tag{A.10}$$

Due to the fact that Minkowski-Hlawka theorem can be proven for Λ_f, the following theorem immediately follows.[15]

Theorem 37. *Let E be a Jordan measurable bounded subset of $\mathbb{R}^{2n}$ and let k be an integer such that $0 < k < n$. Then, for any $\delta > 0$, for all sufficiently large q, and for*

all sufficiently small γ, the arithmetic average of $P_{amb|E}$ over all lattices $\Lambda_f = \gamma \mathbf{B} \Lambda_C$, $C \in \mathcal{C}$, which we denote as $\overline{P_{amb|E}}$, is bounded by

$$\overline{P_{amb|E}} < (1+\delta)\, Vol(E) / \, Vol\left(\mathcal{V}_{\Lambda_f}\right) \tag{A.11}$$

where $\mathcal{C}$ is any balanced set of linear (n,k) codes over $\mathbb{F}_q$ and where $Vol\left(\mathcal{V}_{\Lambda_f}\right) \triangleq \gamma^{2n} q^{n-k}\, Vol(\mathcal{V}_\Lambda) \left(\frac{\sqrt{3}}{2}\right)^n$ is the fundamental volume of the lattices $\Lambda_f = \gamma \mathbf{B} \Lambda_C$, $C \in \mathcal{C}$.

Note that as $n \to \infty$, E will approach the shell of a $2n$-dimensional ball with radius $r_{\underline{z}} = \sqrt{nP_{\underline{z}}}$. Thus

$$\mathrm{Vol}(E) \leq \mathrm{Vol}(\mathcal{B}(\sqrt{nP_{\underline{z}}})) = \frac{\left(\sqrt{\pi} r_{\underline{z}}^2\right)^n}{\Gamma(n+1)} \quad \text{as} \;\; n \to \infty \tag{A.12}$$

which immediately follows that

$$\overline{P_{\mathrm{amb}|E}} \leq (1+\delta) \left(\frac{r_{\underline{z}}}{r^{\mathrm{eff}}_{\gamma \mathbf{B} \Lambda_C}} \right)^{2n} \tag{A.13}$$

as $n \to \infty$. This implies that $\overline{P_{\mathrm{amb}|E}} \to 0$ as $n \to \infty$ for $r_{\underline{z}} < r^{\mathrm{eff}}_{\gamma \Lambda_C}$. Hence for a given lattice $\Lambda_f = \gamma \mathbf{B} \Lambda_C$, $P_{\mathrm{amb}|E} \to 0$ in probability as $n \to \infty$. Taking into account that $P(\underline{z} \notin E) \to 0$ as $n \to \infty$, from (A.10) we conclude that $P_e \to 0$ in probability as $n \to \infty$. This completes the proof.